TO BE RETURNED TO
G.C.H.Q. ARCHIVES
Room C/2504A,
Priors Road,
Cakley,
CHELTENHAM,
Glos.
Ext. 2134.

THE HISTORY OF HUT 6

"Everybody has won, and all must have prizes."

THE HISTORY OF HUT 6

IN THREE VOLUMES

VOL. I

0.0 EDITOR'S PREFACE

The subject of the three volumes of the present work is the history of Enigma breaking in Hut 6; and it is essential, above all, to stress the point that the history is necessarily incomplete and in a sense fragmentary. The whole process of breaking Enigma and using the results obtained is a continuous chain of which Hut 6 was only one link. Other links in the chain were the intercepting stations, both at home and overseas, Sixta and, finally, Hut 3, who assessed and distributed the material presented to them by Hut 6. It is impossible for any reader to comprehend fully the complete picture unless he reads not only this history but also those produced by what we have called the other links in the chain. Moreover, even in certain parts of the present work, a knowledge of certain matters which will be fully described in the History of Sixta - such as German callsign systems- is essential. However, every endeavour has been made not to trespass on the preserves of other sections and only to refer to them so far as is necessary to clarify the mutual relations existing between them and Hut 6.

In another sense, too, this book is incomplete. Much of what would otherwise have had to form a part of the history of Hut 6 has been placed in the separately compiled "History of E/ Breaking, Part II". The reasons for this step are given in the following section on "The Plan of the Book".

Apart from the fact that the present work is in its nature incomplete I feel it cannot but suffer to some extent from the inevitable drawbacks of a work by many authors. The expedient of composite authorship was, however, quite inevitable, as no single person was master of all the subjects that had to be treated. But the various Books are virtually independent entities: and it is hoped that in each case sufficient unity of plan has been attained by assigning the shorter Books to a single author and by planning the longer Books in considerable detail beforehand. It is believed that contradictions of fact have been removed; but it has not been thought necessary to be nicely meticulous in suppressing any shade of differences of opinion, and on certain points - such as, for example, the relative severity of the various crises, cryptographic and other, that shook Hut 6 - divergent standpoints will be apparent to the reader who, with the facts before him, can form his own judgement.

All the authors of this history were members of Hut 6; and the primary authority is simply the personal recollections of the authors. Naturally, however, all the documentary evidence available has been studied: this consists mainly of the regular reports of the Hut, published weekly since late 1941 or in some sections early 1942. Apart from this, special papers and sectional log books have also been consulted.

It will be noticed that for the first two years of the war the documentary evidence available is rather slight, and here in particular we have had to search the recesses of memory. Special difficulty was found to arise with the earliest history of all - that dealt with in Chapter 1·1 - as none of the authors arrived at Bletchley Park before January 1940; and, though we have been careful to consult the few available documents and make enquiries of such personal sources as were available, it remains true that before January 1940 this history rests on secondhand evidence. This must excuse the comparative paucity of dates and occasional

dubiety of minor facts in our prehistory; there is, fortunately, no uncertainty about the main course of events.

The purpose this book is designed to fulfil is twofold. The first is to act simply as a historical record: in the preparation of this work I have noticed how difficult it has proved where no documentary evidence exists to attain absolute certainty on events that happened but five years ago, and, with the speedy dispersal of virtually all the staff of Hut 6, some permanent record clearly had to be compiled at once before the panorama began to dissolve in the mists of the past. The other possible purpose is didactic. I have often felt that it would certainly have been interesting for us (if only for the sake of comparison) if we had been able to consult a history of the achievements of our predecessors in the First World War: and in the same way the present work might be of interest and possibly of use to our successors as, following in the footsteps of Oedipus whom we may claim as the first cryptographer they in their turn strive in their day and generation to read the riddle of the Sphinx.

29th September, 1945.

0.1 THE PLAN OF THE BOOK

The plan of this history appears in detail in the following Table of Contents: but a few general and preliminary remarks may be useful to the intending reader.

The first section after the Table of Contents is a general introduction, a sketch of the whole history of Hut 6, from the pen of the Head of the Hut, P.S. Milner-Barry. This account should certainly be read before the rest of the book is tackled as it gives a delightfully vivid bird's-eye view of Hut 6 and its life. It is true that it contains some technical terms which may puzzle a reader who comes to the History with no previous knowledge of the subject, but the general lines of the story are clear, and any obscure details are best left to be clarified by a second reading when the reader has delved further into the history.

After this introduction the history proper begins. Most of the main divisions or "Books" correspond to the chief functional divisions of Hut 6 and indeed are such as are almost inevitable in any cryptographic organisation. Traffic must be intercepted, then identified, then registered, then broken and then decoded; each of these operations was performed by a separate section of Hut 6 and to each a separate Book is devoted. The order given above (which is the normal chronological order) has been followed except that for obvious reasons breaking the traffic - the end of the whole process - has been placed first. It now remains to discuss the arrangement of the work within the various Books.

Book 1, CRYPTOGRAPHY, deals with the actual breaking of keys and with the work of the cryptographic sections - i.e. Watch, Research and Machine Room. The treatment throughout is primarily historical: after an introductory description of the machine five chapters follow on the main cryptographic periods of the war. Then two shorter chapters deal with the closely related subjects of Bombe Control and the History of the Machine Room: and finally we have a long chapter on the History of Special Groups of Keys and a short final one of General Comments on cipher security.

Technical details and full descriptions of the processes involved have not been inserted in this history - these will be found in the separately published "History of E/Breaking, Part II". There were three main reasons for taking this course.

(1) Even as matters stand, the Book on Cryptography is the largest division of this work, and if full technical details had been added the Book would have reached too disproportionate a length.

(2) It was believed that there would be considerable gain to clarity of exposition if the technical and historical approaches to cryptography were firmly separated and dealt with in separate works. To deal with them in the same book would have meant that confusing changes of standpoint would have occurred rather frequently.

(3) Technically, the problems of Hut 6 were similar in many respects to those of Hut 8. It was possible to bring this out (as has been done) in a joint Technical History but the problems of Hut 8 could clearly find no place in the history of Hut 6.

The result of the course taken is that the treatment of cryptography in the present work is as little technical as possible (with a few exceptions to be later mentioned). This history is, in short, written for the layman who should consult

the Technical History for further details on any point that has aroused his curiosity. On the other hand, the professional cryptographer may well prefer to read the Technical History first, and consult the present work later for the purpose of filling out the historical background.

The exceptions previously referred to are Chapters 1·0 and 1·1. These do contain a certain amount of technical detail and in fact Chapter 1·0 (which contains the unavoidable minimum of information about the machine) is taken direct from the Technical History. Chapter 1·1 deals with the early history of Hut 6 with which questions of technique are so closely bound up as to make impossible the rigid separation that is later enforced.

The only other comment worth making on Book 1 is that the constantly increasing complexity of the general cryptographic situation is reflected in the increasing length of the historical chapters. The stage was indeed crowded for the Fifth Act.

Book 2, INTERCEPTION, is much simpler in structure. The more technical side will be dealt with in other histories and we have only striven to deal with the matter from the Hut 6 point of view. After a general introduction and a chapter on Stations and Communications, there follows a chapter on the routines and history of the Control Room, the Hut 6 section concerned with interception. This central chapter is followed by a shorter one on the rather special subject of Overseas Interception, a few General Comments and a brief Appendix on Hut 6 Liaison with W.O.Y.G. For statistics of sets the reader is referred to the Statistical Appendix at the end of the whole work. It will be noticed that this Book is arranged by subject, and not, in the first instance, chronologically.

Book 3, TRAFFIC IDENTIFICATION, is apart from Book 1, the longest. Its special peculiarity is that it deals almost wholly with the period from November 1943 onwards when Traffic Identification first became a problem and T.I.S. was set up. Again the Book is arranged primarily by subject after a general introduction. The principle has been to describe in the first instance the normal routine of Initial Sorting and the work of the Duddery, then to discuss the more specialised work of Sector Investigation, first on the Air and then on the Army, with illustrations from specific sectors, and then to deal with the two great Traffic Identification crises in some detail. There is thus a steady progression from the simple to the complex. The final chapter 3·9 is in the nature of an Appendix containing a number of papers on special points, some of which are mainly intended for purposes of reference.

The remaining Books are very much shorter and, for that reason alone, have a clearer outline. In Registration and Decoding an attempt has been made to keep the basic routine quite separate from the refinements introduced to meet special problems and circumstances. The Statistical Appendix and Glossary are naturally mainly designed for reference.

It should perhaps be emphasised that the Books are to a great extent independent and though the order adopted seemed to us the best there is no very cogent reason why the reader should not pick and choose among the Books to suit his taste. But it is certainly advisable to read through in order whichever Book is chosen.

CHAPTER 0·3

HUT 6 : AN ADVENTURE

0·30 GENERAL RETROSPECT

So much has happened in the past five years, and at such a pace, that much of what happened, especially in the early days, is hidden in the mists. It is difficult even to recall the atmosphere in which we worked, let alone actual events or incidents in any sort of order. The story, both on the technical and historical side, is set out by various hands, all of them much more capable than I should be at describing the work and the fortunes of their own sections. All that I can try to do is to sketch very briefly and in the broadest outline the picture as a whole, to trace the development of the organisation, selecting what seem to be the most important points and pointing out the mistakes that we made. Even this will be a very partial and one-sided affair, for I shall only deal incidentally with the other members of the Enigma combine - the stations, Sixta, the bombe huts, Hut 3. The whole process formed one whole and Hut 6 had to have the closest and most intimate relations with all of them. The longer the war went on and the more difficulties the Germans put in our way, the more our affairs became mixed up together and the closer the collaboration had to become. That held good just as much for our external relations as for those between the different departments of Hut 6; but this story does not pretend to be more than the story of Hut 6. The work of the intercept stations and of Sixta in particular seems to me to have become steadily more difficult and more important in relation to the whole, particularly in the final stages, and this ought as far as possible to be borne in mind in reading the following pages.

There is a further caution which I would like to give. I was intimately concerned with the beginnings of the Crib Room, and, as it later on developed, with the Watch; and only became Head of the section in the autumn of 1943. What I have to say about the first four years, then, is inevitably written from rather a narrow standpoint; in particular I had little or nothing to do with the development of interception or with that of what was known as "W.T.I." and subsequently grew into Sixta. That was Welchman-Colman, Welchman-Blair Conyngham and subsequently Welchman-Lewis. The struggles to obtain adequate interception facilities went on unremittingly for the first few years of the war and they were, of course, vital to the ultimate success of the firm. But the main part of that battle had been won by the time I took over. Again, it was Welchman with his strange and uncanny knack of grasping the ultimate significance of things who fought throughout for the recognition of the importance of "W.T.I." Many of us, myself certainly included, thought that this was just a fad, and it is in fact true that the cash value as an aid to breaking of the whole log reading and Fusion Room organisation in the first few years of the war was extremely meagre. In fact, in my view, we could have done perfectly well without it. But Welchman's prescience was to be brilliantly justified after his departure, when the knocking down of the various props which had made identification almost a rule of thumb matter - first discriminants, then changing frequencies and finally encoding of callsigns - made the cryptographer largely dependent on the complete and accurate knowledge of the German W/T organisation which Sixta had steadily been building up. Then what had been from the cryptographers' standpoint a luxury became a basic necessity of life and, if Welchman had not fought for its development in the early years, we should have had no hope of weathering the storms which nearly overwhelmed us in the last eighteen months.

However, if one was not at the centre of things and therefore could not have a proper overall view, the Crib Room was the next best place to be. Just because we had no identification difficulties to speak of, breaking really was a matter almost entirely for cryptographers. At first it was cillies, but with a tightening of German security regulations on this side, cillies were largely superseded by cribs, which became and remained to the end the standard method of breaking Enigma keys. So the Crib Room, as it then was, was in the key operative position, and to concentrate in the early years on the cryptographic side of things should not produce too distorted a view. Moreover, it was a logical function of the Crib Room, as the chief breaking agency, to take charge, under Welchman, of bombe policy generally and of our relations with Hut 3 and with the naval sections. These were and remained the most important matters of general policy to be decided. They were perhaps more crucial, though simpler, in those days. There were far fewer bombes in proportion to the work to be done and therefore, though there were far fewer keys, there was a much more serious tug of war between them. Later on there were so many bombes that even with a much greater number of keys and a much heavier programme of work there was much greater play, and the chance of a really serious clash between vital operational keys (e.g. a Russian convoy and a decisive battle in Egypt) were greatly reduced. 1942 and 1943 saw the development in embryo of the liaison between cryptography and intelligence, which was developed to a high degree of sensitivity under Manisty as head of the Watch.

I shall say next to nothing, too, of the technique of bombe design nor of the battles which were successfully fought to provide us with enough tools to do the job at the breaking as well as at the intercepting end. That again, under the Director, was almost entirely Welchman's achievement, not only when he was Head of Hut 6 but when he was translated to a higher sphere. It will be clear, I hope, that alike in interception, in W.T.I., and in the production of high-speed machinery I took over in October 1943 a concern in which all I personally had to do was to see that proper use was made of the tools which the foresight of others and especially my predecessor had provided. Many dramatic and spectacular events occurred in the final eighteen months, which make them one of the most exciting experiences it is possible to imagine. But the spade-work which enabled us to emerge from them in good shape had all been done long ago.

0·31 1940

To go back to the beginning, which from my point of view is February 1940, some time after the first break had been made (on the old indicating system, by means of females). It is not at all easy now to recapture the atmosphere of those days. The main sensation of the bewildered newcomer was that he was participating in a miracle which he was entirely incapable of comprehending. I may say that this sensation has never entirely left me and that no amount of success staled the thrill of a break, be it on the most cast-iron crib or the most obvious of cillies; that is no doubt the advantage of a non-mathematical mind, which is incapable of grasping how man or machinery or both combined can possibly find the right solution out of 150 million million (is it ?) possible answers. However, breaks were certainly occurring, though hardly on an operational basis. The traffic was mostly days or weeks old and very dull at that (quite trivial on Red or Blue); but even to

the least imaginative it was obvious that the enemy was not perfecting his wireless technique or exercising his cipher operators for fun. This was the considered opinion of Hut 3 (total strength, Saunders, Edgar, Lucas).

Nevertheless, it was an act of faith to put the Hut on a 24-hour basis. This was done chiefly to avoid the Registration Room having an accumulation of some 15 hours' traffic - 6 p.m. to 9 a.m. - to deal with in the morning. But I can still remember Welchman talking about "dealing with the traffic on an operational basis" at a time when the "phoney war" was still in progress, and when the terms carried no significant meaning to me.

Nor did they to the higher authorities (I do not of course refer to the present Director). The innovation was thought to be not only a strange fad, but dangerous to the morals of a mixed community. Indeed a total of three girls (which was all that we required) was thought to be insufficient to ensure the observance of the proprieties; and presumably on the principle that the men would be overworked by such large numbers, a minimum of six was insisted upon. It was therefore necessary to bring in three unfortunate members of the Netz Room to act as dummies, a precaution which was dropped by tacit consent after a short interval. The experiment was duly launched and was a great success. Several of the original members of that shift - David Gaunt, Michael Banister, Sheila Dunlop and June Carney, remained with us to the end, or almost. And very good fun it was, cooking eggs and bacon in the kitchen ourselves in the middle of the night with copious draughts of tea and unlimited jam.

And it was also very fortunate or very providential because no sooner was the night shift in full swing than the Germans invaded Norway. Traffic jumped up on a new key, Yellow, and we found ourselves breaking currently. However, our triumph was short-lived because, although we lasted out the Norwegian campaign, and the intelligence content immediately verified the predictions of Hut 3, the Germans then changed their indicating system and Hut 6 met with its first and last check in the continuity of breaking, at any rate on the main Air Force keys.

I can remember most vividly the roars of excitement, the standing on chairs and the waving of order papers, which greeted the first breaking of Red by hand in the middle of the Battle of France. It was never surpassed, and equalled only I think by the first breaking of Brown later on in the year. In later times the nearest approach was the first break of Light Blue in (I think) March 1941. This occurred when the first party of American visitors was being shown round Hut 6 and must greatly have astonished any of them who had the idea that the British were a phlegmatic race. Highlights of this kind were naturally rarer in the modern age, but, though sentiment was more restrained, a good deal of the same underlying tension communicated itself when Oliver Lawn broke Uncle D in the small hours of January 2, 1944 - a shortlived triumph, but an extremely dramatic one. (Welchman and Rees achieved the same feat with the mysterious Uncle Charlie, also on the night shift, in bygone days.)

However, naturally this first break of Red was the greatest event of all, because it was not only, in effect, a new key, which is always exciting, but because we did not then know whether our number was up altogether or not. The first bombe was not yet in action, nor had cribs as yet been thought of (except probably in

the fertile imagination of Welchman, ranging as usual a long way ahead of the event). So the break had to be by hand on new technical methods invented by the experts of the Machine Room. As was to happen again and again, we were assisted at precisely the right time by the enemy, because this was the heyday of cillies and of the ringstellung tip (the "first message" cluster) without which hand breaking would have been impossible. The W.R. experts proceeded to hit sixes all round the wicket for the rest of the Battle of France and part of the Battle of Britain.

The volume of traffic on the one key was enormous - over 1,000 messages one day, which was broken at 9 a.m. I cannot now imagine how, with our primitive methods of collecting and registering traffic, and our tiny staff for decoding it, we managed to cope at all. Anyway, the job got done somehow, the Battle of France was lost, the miracle of Dunkirk occurred, the Battle of Britain was won, and Hut 6 settled down for the winter. Not, however, before the threat of invasion had caused plans for a mobile Hut 6 to be far advanced, and even the team selected. The selection of a very small team of girls from 100% volunteers caused almost the most serious crisis in our personal relations that I can remember. Fortunately the emergency never came to pass, for I really think that those excluded (in nearly every case on grounds of physical condition alone) would have stowed away in the lorries rather than be left behind.

The dying down of the battle was followed almost immediately by a marked improvement in German security, and the autumn of 1940 witnessed the birth of the Crib Room. I had been entirely sceptical of the possibility of ever finding or recognising standard routine messages of the requisite length, and only the persistence and optimism of Welchman, independent as it seemed to me of any evidence, induced me to make the attempt. We then set up the C.R. by removing the young men from the Registration Room, leaving the young men in the Machine Room to carry on the more technical machine side of breaking, including bombing, finding ringstellung, etc., as well as cillies and hand attempts. The arrangement most unfortunately became crystallised, and a disastrous and, as it ultimately proved, quite unnecessary split was created for which I must take the chief blame. I will say something more about it and its consequences later on.

The remaining major cryptographic event of 1940 was the breaking of Brown and its exploitation as an operational key. Nobody knew what its contents would be and the most extravagent hypotheses were entertained. It proved a delightful and most entertaining key cryptographically, because although the traffic was small the density of cribs and of cillies was phenomenal. Never before or since have so many and such gross breaches of the most elementary rules of cipher or procedural security been committed as by the specialists of beam bombing. They never learnt and the Germans signals officers apparently were powerless to intervene. It was also extremely exciting, because of course the object of the exercise was to discover the target before it was too late to be of use to the Air Ministry. The breaking of Brown, moreover, gave us our first insight into the necessity of close liaison between intelligence and cryptography, because we had to decide whether we would put all the (two or three) available bombes on the full range of wheelorders, starting early in the morning on the overnight cribs; or wait until two or three messages were gathered together, after which it was any odds that cillies would effect a substantial reduction in the wheelorders. The first course was

[illegible] election by extravagant, but gave a much better chance of getting the result in time. It meant having [illegible] later on Light Blue (7.45 in Attic) to take out [illegible] will later in the day, [illegible] through they might be. [illegible] the idea of Hut 6/Hut 3 [illegible] Dining, though [illegible] [illegible] [illegible] divided [illegible].

[illegible]

[illegible] of course, was [illegible] in history. Never again [illegible] quite the same sense of fighting for our lives, because however bad things were later [illegible] in the street [illegible] the life or death [illegible] fighting was never quite repeated. Typographically, too, 1941 was a comparatively uneventful year. It dribbled down to a routine of trouble. Red on white and [illegible] was joined by Light Blue, the initial breakthrough and exploitation of which was very exciting. All the same, all through this great time persisted, at any rate in my own mind, the sensation that it was all much too good to be true, that any day now the enemy would discover and that we should wake up one morning to find that it was all over. In retrospect one sees these fears to have been much exaggerated, but the technique of cribbing was in the early stages and already appreciated what a powerful weapon was being forged. Moreover, our fears were justified to the extent that for a short period in the autumn it really did look as though we were in imminent danger of losing both Red and Light Blue. For some time we hung on to both by the slenderest threads. In those days the effects of getting into a jam were much more noticeable than they were later, by which with only two or three keys work simply came to a standstill if nothing broke for a few days, and the whole Hut descended rapidly into the darkest abyss of despair. It was almost worth [illegible] into the abyss, though, for the pleasure and thrill of emerging from it. It would always happen that everything came right all at once, a whole series of hut days would [illegible] and everybody [illegible] on it. One of my most vivid recollections of those early days is of listening anxiously as [illegible] the [illegible] of the dawning realized [illegible] [illegible] [illegible]

another recollection of that year is of incredulity at hearing my own voice say "10, Downing Street" to a taxi driver at Blackfriars and arriving unopposed - the first and no doubt the last time that I shall find myself inside those doors. It seems a long time ago now.

1942

1942 was the annus mirabilis. In the beginning of that year the Germans suddenly realised that there was no objection, and obviously great advantage in security, in using a large number of different keys for the different major units of the G.A.F. However, with characteristic blindness the enemy undid much of the good that this step might have done him, for instead of making up entirely separate keys he subtracted old ones in a delightfully simple plan which the ingenuity of Mr. Parker soon uncovered. The effect of this was that, every other month, the majority of Air Force keys were in our hands for the decoding, and a tremendous boom ensued which taxed our resources to the utmost. In June the D.N. was decoding 1170 messages a day (about half the figure for the closing months of 1944). In August over 500 breaks were made, double the previous best, and 50 keys in all were recognised. This result was achieved on the ridiculous total (by subsequent standards) of 29 bombes. By October the worst of many major crises had arisen in the D.N. and the R.A., but we were eventually saved by the autumn influx of university candidates and the setting up of schools to train them.

Not only was there all this commotion on the Air side, but 1942 was the great year of the African campaign, culminating in the battle of Alamein and the long retreat of Rommel towards the final catastrophe in Tunisia. It saw the development of an entirely new technique, that of re-cribbing; for the Army keys in Africa split into several components, and all of them were closely interconnected. Here again for a long time I remained very sceptical about the practicability of ever making use of re-encodements, on the grounds of variations in spelling and abbreviations etc., change of address and other alterations. Dudley Smith, who at that time constituted the "O.N. Research" section - a new and important innovation - worked away a long time at re-encodements between, I think, Gadfly and Chaffinch. Eventually the long awaited breakthrough in April was made by Banister guessing a straight segment, but Smith, who had been confident always that the re-encodement method could be made to work, was, certainly most unlucky. He was baulked on one occasion by the ill luck of a corruption in the original Gadfly text from GAMMA to PAMMA, in a context where PAMMA made equally good sense and was passed without comment by Fr. L. If the corruption had been to any other letter than a P the encodement would no doubt have been made. Moreover, the Russian cribs' mistake effectually prevented any possibility of obtaining the correct solution on the Chaffinch, because in the right position the bogus P crashed with a P in the Enigma text. I mention this in some detail because it seems to me a classic instance of the part played by luck in our affairs, and because it might so easily - though in fact it did not - have delayed by weeks our re-entry into the African Army keys at a most critical period. One could, of course, easily name equally extraordinary instances in which the luck ran in our direction, and with equally providential consequences.

Be that as it may, the re-encodement technique had clearly come to stay, and in fact there proved to be no more interesting and enjoyable side to cribbery. In passing, it is worth remarking that of all the egregious errors committed by the Germans, the folly of sticking the same time of origin in the preamble of two encodings of the same message was the worst. It enabled us quite gratuitously to pick up the vast majority of re-encodements on "kisses" - the comparison of G.T.&C.'s between messages on different keys. They thereby reduced what should have been principally a W.T.I. job - the comparison of routeings - into a largely mechanical routine operation; though, of course, knowledge of callsigns, units involved etc., was still highly desirable.

The Chaffinch pot boiled away merrily all the summer and autumn and there were several vitally important operational G.A.F. keys as well, such as Red, Primrose, Locust and Scorpion. (The last one named was front-line tactical matter of the highest degree of urgency, but it providentially repeated the Primrose key of the preceding month. This enabled us to send the keys out to Africa, and to have the traffic decoded on the spot from messages intercepted locally.) The C.R. became a hive of activity and it was necessary to expand it very quickly. It was about this time that the experiment was tried of promoting from other rooms, such as the R.R., the best available girls. This experiment, frowned upon by the more conservative, proved an immediate success; but it still further increased the discontents of the Machine Room cryptographers, who in the absence of cillies or hand attempts or other suitable material for their virtuosity found themselves more and more in the position of hewers of wood and drawers of water for the C.R., who were having all the fun. However, the business of the key repeats, which by our then artificial separation was a M.R. function, served to disguise the fact that an untenable situation was developing.

It was during this summer that the intelligence liaison with Hut 3 was put upon an organised basis by the setting up of 3 L. It was the first time, I think, that a definite attempt was made to guide the Hut 6 effort by the light of known forthcoming Allied intentions. This was the effort to get a grip on Locust well in advance of the August convoy to Malta. As I remember we were not on this occasion told the nature of the forthcoming operation, but later on - I think first on the occasion of the African landings, in which Locust was also in the forefront of the battle - the broad character of the operation was revealed to senior officers in Hut 6. This was an essential step for the intelligent direction of cryptographic policy. The liaison thus established worked almost without friction or serious disagreement, with both parties on an equal footing, until the end of the w.e. It would be impossible to overrate its importance in the combined Anglo effort, but it worked so well that it has virtually no history.

At the same time more systematic consultations were arranged with Hut 8 and Block A (Naval Section). There was danger of really serious conflict of claims here, because there was no overriding intelligence authority that could balance the claims of the Admiralty against the War Office, and we had to work out our own solution. It was a question of the best use of the bombes at a time of the greatest stress, with the U-boat warfare at its peak and the decisive battle being fought in Egypt. The decisions, which had to take account of highly technical considerations, could only be taken by the man on the spot in the light of the best intelligence advice he could get. We solved the problem by setting up a rota of bombe directors or dictators from Hut 6 and Hut 8, who had plenary

powers during their turn of duty for deciding on the distribution of the bombes. We were very lucky that the really crucial occasions were so rare, but the decisive factor in avoiding serious confliot of opinion was the broadmindedness and clearheadedness of Alexander, the Head of Hut 8. The directors seemed to me to vary considerably in the calibre of their judgment, but they all did their best, and decisions were rarely if ever taken on what might be called party political lines.

The problem became less acute as the output of bombes increased. The naval keys did not proliferate like the Army and Air Force and therefore the total requirements of the Navy loomed less large. Nor did they grow more difficult as did those of the Army. In the end it was almost always possible to find bombes without more than temporary inconveniences for urgent naval demands, and it became possible to disband the directors and put the problem on a basis of long-term discussions of policy. This was done by holding weekly meetings at which intelligence and cryptography from both camps were represented, and broad lines of priority were agreed upon. These meetings too were a success, and occasions of serious disagreement hardly ever occurred. This again was due to the fair-mindedness and impartiality of the intelligence representatives. I usually felt that they leant over backwards in their determination to give full weight to the intelligence needs of the other services.

1942 ended with the tide of battle definitely turned in favour of the Allies. The landings in Africa had been successfully carried through, and the stage was set for the final battle of Tunisia. The last month of the year, however, was marred cryptographically by the arrival of wahlworts or nonsense words on the Finches, not apparently a general security measure but the invention of some local security officer in the Italian theatre. They were clearly destined to prove a major obstacle to breaking, because though they set no intrinsically new problem they enormously multiplied the job to be done. They meant running a crib perhaps in several different positions, or perhaps several versions in several positions, instead of one version in one position. This could be overcome, in theory, by a sufficiency of bombes, but until the supply of bombes, particularly of Washington bombes which could run shorter cribs, caught up with the demand, we were bound to be seriously handicapped.

0.U. 1941

As 1941 to 1940, so 1943 to 1942 was something of an anti-climax. It was very much of a transitional period in many respects. Key repeats in the Parkerian sense ceased, and the breathless pace slackened. Old Hut 6 finally burst its bounds and in the spring we moved into our palatial new quarters in Block D. At first we appeared to rattle about like peas in a pod, and it seems fantastic to suppose that within a year or so we were again clamouring for more room and knocking down walls to provide it. We were still digesting the autumnal influx of new staff. The African campaign lasted till May and the Finches ended up in March with a blaze of glory. In April they became virtually unbreakable, and the decision was taken in consultation with Hut 3 to abandon the impossible task of trying to break Bullfinch and to concentrate on breaking new ground in preparation for the next round. By that time the battle was clearly won, and it did not matter whether we broke it or not. Hut 6 for prestige and Hut 3 for news interest would no doubt have liked to pursue the Finch to the bitter end, but it could not be justified on grounds of strategy.

The most important event of the spring was the setting up of the Watch by the amalgamation of the M.R. and the C.R. and the setting up of a separate Research Section on a considerably larger scale. (Both M.R. and C.R. had had their own Research Sections for some time previously, for the investigation of unbroken keys or the exploitation of non-operational ones. But this was a new unified organisation under Major Babbage.) There is now little doubt in my mind that it was a mistake not to have done this earlier, but the reasons were not purely historical or conservative. It had been argued by the supporters of the status quo, on the one hand that the C.R. were not mathematically minded and would therefore be ill-fitted to cope with the more technical aspects of the machine; and on the other that the M.R. were mathematically minded and were therefore not likely to be proficient at cribs and re-encodements, which were thought to require a linguistic or humanitarian background. There was an element of truth in this reasoning but also a good deal of prejudice on both sides. The M.R. undoubtedly felt that with the gradual lessening in the importance of their side of things they had been elbowed out, and were now being deliberately kept out, of the more entertaining aspects of Hut 6 cryptography. The C.R. reacted against what they took to be an unjust aspersion and partially justified it by standing somewhat jealously on their privileges.

The decisive argument in favour of the change was that it was absurd and uneconomical to have one man finding a crib on a key and solemnly passing it to another expert to find the cillies. Great saving of labour and efficiency would be achieved by having the complete handling of a key done by one man; and even had the logical case not been so strong the psychological case for removing the M.R. grievance was overwhelming. It is quite arguable, I think, that we were so busy during 1942 that a large-scale change of this kind could not have been effected without considerable sacrifice of exploitation; and that we did all that could then be done, by having visitors from the M.R. for courses in the C.R. as opportunity offered. However, the setting up of the Watch, which was Welchman's last major reform, produced an immediate and permanent improvement in the atmosphere which ever afterwards became, I think, quite as happy as that of any Room in the Hut. The main damage was that it came too late to restore the morale of one or two very able members of the M.R., who went off to do outstandingly valuable work in other sections. It was soon found that the mathematical education was as good an any other for cribbery and re-encodement work; and that those unversed in the mysteries of mathematics could nevertheless make a surprisingly good showing at the more technical aspects of machine cipher, though naturally they could not rival the experts in this sphere.

Now up to this time - say the spring of 1943 - Research had been something of a poor relation. Certainly it was not so in the eyes of Welchman, who always saw the long-term importance of things more clearly than anybody else. But the main weight of Hut 3's interests lay naturally in the operational keys on which immediate action could be taken, and my own bias was certainly in favour of the immediate and urgent objectives as against the more remote. Therefore, with a limited amount of bombe time available, the difficulty had always been to see that Research keys, whether being handled by M.R. Research or C.R. Research, did not get squeezed out altogether. I do not think, in fact, that we made any unfair distribution, or that we could have devoted substantially more time to Research than we did, without adversely affecting operational work. But I am very conscious that the inhabitants of the Research Sections must have felt that they were ploughing a

lonely and unappreciated furrow. From time to time we made the experiment, regarded as a pretty daring innovation, of allocating two or three bombes as a definite minimum for Research work, and in this way we usually managed, even at times of the acutest stringency, to keep the flag of Research flying. But for long periods we barely achieved even that.

In the early spring and summer of 1943 all this was changed. With the collapse of resistance in Tunisia our main theatre of operations closed down and did not reopen till the invasion of Sicily and the mainland. There were not wanting those who said, not for the first time, that the great days of Enigma were over: that, with the Germans forced back into fortress Europe, and eventually into their own territories, they would have less and less need to rely on wireless as their main channel of communication: that Fish would supplant Enigma as the vehicle of all high-level strategical material, and so on. All of these predictions were to be gloriously falsified in the great days of the invasion of Italy, of the second Battle of France, and of the final Battle of Germany. But in 1943, while we were waiting for the move into Sicily, there was certainly a lull; and this was clearly the time for switching our main attack on to Research keys, especially Army keys, with the idea of finding out anything and everything that we possibly could about the strength and dispositions of the enemy in Europe. There were, at this time, very few operational keys left - only three or four - and therefore, the newly-founded Watch had a very lean and depressing time, which tried everybody's morale as highly as 1941. What we did, therefore, was to transfer a considerable number of cryptographers to the Research Section. It had for a while all the bombe time it needed and made very good use of it. Taunt and Roseveare were the leading men on the G.A.F. side, Gaunt and Nicoll on the Army, with Babbage and Aitken as the senior partners.

By this time we had developed a sound and flexible organisation for transferring keys from one category to another. The general principle was that a key was handled by the Watch - i.e. on a 24-hour basis - if (a) it had operational urgency and (b) it was currently breakable. If it was currently breakable, but not important enough to break every day or extravagantly, it was handled by "Research" - in this sense an obvious misnomer; and similarly however urgent or important a key was, there would be no sense in handling it in the Watch if it was not currently breakable. Keys of this type, therefore, were handled by Research, more patiently, and in a calmer atmosphere. The division of work between the two Registration Rooms corresponded with the allocation of keys as between Watch and Research at any given time. Incidentally the qualities required for dealing with keys in the Watch are largely different from those needed for Research, and this imposed a limit on the freedom of movement of cryptographers from one section to another.

One disadvantage of this constitution was that, except at rare intervals such as the summer of 1943, the transfer of keys was largely one way. This, of course, was inevitable. As soon as a key developed operational urgency, and became breakable through the efforts of Research, a claim would be put in by the Watch to have the key transferred. It thus appeared that Research did all the dirty work, and as soon as their spade-work had been crowned with success, the baby was snatched from them. I, as Head of the C.R., or the Watch, appeared to be greedily grabbing keys from Research just as soon as they began to look really interesting and to become good fun cryptographically. Claims of this kind, however logical and inevitable and even if admitted to be so, could hardly

be put forward or strongly pressed without a good deal of heart-burning, particularly when the claimant was the man who was going to have all the fun. Among many instances of this one of the clearest was the transfer of the Finches to the C.R. in May 1942, just before the Kammal offensive, a short while after they had been resuscitated from the grave by Bradley Smith and Sandstar. I think if one were making a blue print of a constitution, and not dealing with a live organisation and a process of evolution one would avoid difficulties of this kind, which could easily have led to time-wasting delays, by putting the whole cryptographic effort under one head: so that a decision would be taken in one man's mind rather than on arbitration between conflicting claims. That no serious delays or damage was caused, even though the arbitration nearly always had to be one way, was due to the essential reasonableness and broadmindedness of the Research party and the loyalty with which they suppressed their own feelings. In the end, after a further process of evolution and in very different circumstances, we did achieve what appeared to be a more logical and satisfactory structure; but of that more hereafter.

However that may be, it was a good thing that the lend-lease worked in reverse in the summer of 1943. Indeed the heyday of Research really lasted until the spring of 1944, though naturally the invasion of Sicily and subsequently of Italy in the autumn of 1943 brought the Watch to life again with a jerk. There was plenty to do then, because Army keys, such as Albatross, Cormorant, Shrike, and subsequently Bullfinch, were mostly extremely difficult. Their expensiveness, combined with that of Army Research, was such that for a time at least in September Air Research had a lean time, and a system of rationing had again to be adopted. This again was an inevitable consequence of the fact that the emphasis of intelligence leant more and more heavily in the direction of the Army. It was the Army that we had to meet and beat in the field before we could finish the war, and G.A.F. keys were prized more and more for the light they could throw on the Army than for any intelligence they could give about the outclassed G.A.F. This situation was accepted and understood by the Roseveare/Taunt combination. They pursued an essentially secondary rôle with the utmost vigour. Fortunately I was able to assure them honestly that we should all be fully operational in the final stages. (In any case the strength of the G.A.F., or at any rate the value of intelligence about it, was seriously undervalued at headquarters. I noticed no lack of anxiety about the strength, dispositions and intentions even of a depleted G.A.F. around D Day, nor even as late as the eve of the Ardenne offensive.) It was a great advantage at this stage and right up to the end to have daily contact with 3 L. They sat in on the daily meetings which we held every afternoon to consider and arrange in order of priority the material produced by both branches of the Research Section, and to relate it to the probable demands of the Watch keys. In this way we had the benefit not only of day-to-day tactical advice on the varying merits and urgency of keys, but of long-term views and assessments by which cryptographic policy and effort could be guided.

In October Welchman became sick (Tel.) and I took over as Head of Hut 6, leaving the Watch in Denniston's hands. All that I need say about this is that I could never have given another thought to the Watch either in organisation or on the side of 3 L policy; and this though the last 18 months, for the Watch as for all other sections, brought a host of new problems. Its efficiency and happiness were equally assured. This was just as well, for my attention was violently distracted by a storm which blew up in a quite unexpected quarter.

It was in September that the Germans almost without warning dropped discriminants from Army traffic, thereby destroying our main means of identifying the key. Now discriminants and the whole business of unidentified and dubiously identified traffic had been the province of a few highly skilled specialists with - as was proper for their job - very much of a "research" outlook. This was appropriate to a small percentage of unidentified traffic, but quite different methods and attitudes were required when it was a case of dealing in bulk with a large mass of traffic. What was wanted now was not the patient investigation of each piece of traffic by highly skilled workers, but a bigish organisation which could formulate rules for identifying the great majority of the traffic correctly. For unidentified traffic, if we were not to be swamped, was to hold the problem again to the routine identification of traffic by rule of thumb methods; to be prepared to sort a lot of traffic wrongly, provided that it was sorted somehow. It is no disparagement to the experts who had so far been charged with the investigation of unidentified traffic to say that they were not fitted by temperament to deal with the new situation, any more than one could have transformed the whole Research Section into the Watch, or vice versa.

Now for some reason, all most blindly, we failed properly to appreciate that what the Germans had done on the Army they would almost certainly do later on the R.A.F., a vastly bigger problem because of the far greater volume of traffic. Nor did we take at all adequate steps to see that the Army were managing all right with their problem. Apart from any other considerations, the existing staff was ludicrously small for the needs of the new situation, and almost too small even to form a nucleus for training purposes. The experts did their best and worked all hours, but they were overwhelmed. This was the situation when we had about a week's warning at the end of October that discriminants would be dropped from the G.A.F. at the beginning of November. We had had two months in which to prepare and had wasted them. We never made the same mistake again.

In my opinion, this was easily the most dangerous period we ever went through. It would take far too long to describe even in outline the measures which were put into force, nor how they were just in time to be effective, before the flood of unidentified traffic at the beginning of November swamped us. There was only one man with the quickness and clearness of brain and the originality of mind needed to construct a new framework, and that was Davies; and only one man who could get all the tools together, dot the i's and cross the t's and actually put the thing into operation, and that was Gaunt. These two saved the situation and no other pair could have done it, nor I think either of them alone. But it was a nightmare to live through. I should certainly not forget that Winton, when I had to ask to stand down in favour of Davies, could not have responded more loyally both then and later. But naturally his own staff felt that he had been badly done by and a great deal of unavoidable bewilderment was caused. It was much the most disagreeable decision I have ever had to take, but not the most difficult, because I had no doubt whatever at the time, and have had none since, that it was the only possible one.

Anyway, a new section was built up with an auxiliary called the "Dudley Index" run by David Gaunt - which in effect covered the identification of the Hinton keys. The principle and methods of identifying by frequency and callsign were not, I think, difficult, but there was enormous lot to be done in the way of training the staff and codifying the routine. All this will no doubt be dealt with by the proper authorities in time.

own sections. An incidental effect was that the whole of the new staff collected in the autumn in preparation for the second front was swallowed up in the increased complexities both of identification and, consequently, of decoding. But by the end of the year the crisis was definitely over, only to be succeeded by a new and still more formidable enemy, that of Uncle D.

Off ... 44 !

By comparison with 1944, everything that had happened since 1940 seemed almost tame. It included January 1st, the cheap, unlooked for, and illusory triumph over the Uncle: April 1st, the change to the F book which in spite of months of preparation almost knocked us out in the first 48 hours; May 1st, the famous "damp squib" stocker change to much dreaded in advance; Enigma Uhr, D Day itself with all that it meant in the months of preparation before and the enormous explosion of traffic afterwards; the Battle of France with the Western Army keys coming into their own at long last; August 1st, the culmination of months of sinister distribution of Uncle E; the invention of Dumma to cope with Uncle D, and other D-breaking machinery; the autumn slump when we realised that the war was not over; November 1st, the encoding of callsigns by the Army so ostentatiously handled by Beaumanor. A year which nobody with imagination could ever forget, but one which is such a crowded canvas that within the limits of this survey it is quite impossible to deal with it except in outline.

Let us first dispose of Uncle D. The most elaborate preparations were made for a massed hand attempt on the assumption of a total introduction of the new reflector on January 1st. As is well known, the Germans handed the wiring to us on a plate by using B and D indiscriminately with the same key - an egregious mistake in which they persisted to the end, though as the supply of reflectors increased it happened from time to time that a key was wholly or almost wholly using Uncle D. In nothing were we more fortunate than in the misuse which the enemy made of this decisive weapon. Anyway, we scored our dramatic triumph and breathed again, but not for long. For to our horror a new reflector appeared after ten days, another ten days afterwards, and so on, until eventually we became convinced that the reflector was pluggable. Up till August, its use was extremely restricted - only on a part of Hut 6 - but from April onwards sinister references appeared to a projected extension of the range, and we waited in monthly expectation of snuffing out. However, not passively. Many heads had worked on the problem of devising mechanical means of combatting the monster, and eventually various possibilities were thrown up, three of which - Giant, Dumma, and the Arlington Autocricher - did noble work. Throughout this period we owed much to Alexander, the Head of Hut 8: the whole Uncle D campaign on all fronts, including new and improved versions of the hand attempt, was guided by him as chairman of the U.D. Committee. It was one of his greatest services to Hut 6. For months it seemed that we must lose the race, that devastating extensions by the Germans must take place long before the counter-machinery was ready. To the anxious spectator our progress (though probably spectacular) was maddeningly slow, but the enemy was also (though he too may have been distributing as fast as he knew how) extremely dilatory; and what was more important, when the dreaded extension took place in August, it was on the same stupid lines as the original introduction. All the same, misandled as he was, Uncle D

remained a major and increasingly serious menace, though not till April 1945, when it was too late to matter, did he threaten actually to unfasten our grip on the main operational keys. In the meantime Duenna and her allies did all and more than could have been expected of them, though all turned out their services were not required until the end in the most total fashion. But in April 1944, all this was hidden in the future, and dread of Uncle D was one of the major preoccupations of the year.

Next, the F book. It was known that the Germans were preparing to substitute the F book at midnight on the third book, and after the hideous experiences of the dropping of discriminants we were determined not again to be taken by surprise. The effect of the change was, of course, that until we had got the hang of the new F book allocation, we could make no use of predicted callsigns, on which our whole sorting system was now based. On the other hand we could expect that within a matter of weeks, provided we could go on breaking, we should accumulate enough data to work out the new system and be back where we were before. It was therefore essentially a temporary crisis, though liable to be very fierce while it lasted.

Very elaborate - too elaborate - plans had been drawn up, but even so we were knocked off our balance by the sheer flood of unidentifiable traffic which poured in upon us. The plans therefore broke down, and a state of chaos threatened and for some most unpleasant hours actually reigned. Even now I am not very clear what were the precise measures which we took to restore the situation, beyond ruthlessly scrapping a lot of our carefully prepared machinery which proved to be too cumbersome. But somehow or other the crisis passed of itself, and matters improved very rapidly. This experience taught all of us some invaluable lessons, which enabled us to deal with the intrinsically much worse crisis of February 1, 1945, (G.A.F. encoding of callsigns) in every way more calmly and competently. It taught us to make our plans as simple as possible, or if they could not be simple at least to scrap too soon rather than too late; and above all to make sure that as many people as possible of those who would actually have to operate the plans should have a hand in the drafting of them, and should clearly explain them to their colleagues. These precautions we had not taken thoroughly enough, and we paid dearly for lack of them.

The other distinguishing feature of this episode was that we were brought for the first time into the closest contact with Sixta on an operational basis. As I said in the introduction, in my view the contribution made by Sixta increased enormously in the last 18 months, and became a vital factor in a sense in which it had not been previously. As soon as discriminants were dropped, T.I.S. as an organisation for the sorting and identification of traffic was relying upon - was turning to operational use - the background of knowledge of the German Order of Battle and W/T system which Sixta had built up and it could not have functioned without Sixta. Now, in the F book crisis, Sixta once along and showed us how to identify units and subscribers with the callsign prop knocked away: a tour de force which they did not have to perform for many days, but which they were destined to have to adopt as part of their normal routine when the encoding of callsigns brought us to our final test.

And finally, the F book crisis demonstrated once more that the Watch could rise superior to any difficulties of breaking, as they were to demonstrate once again in the very different conditions prevailing after D Day, and the much more long drawn out crisis

of February 1, 1945. It is said, indeed, that the Watches in Hut 3 noticed nothing abnormal in their supply of intelligence, at a time when the scene of excitement and confusion in R.R.1 defied description, and would certainly have shaken even the imperturbable Group Captain, had he had the misfortune to witness it.

To come back now to May 1st and that which in all the alarms and excursions of Uncle [illegible], Enigma Uhr, dominated all our thoughts and plans during the early months of 1944. I have already set the difficulties of identification swallowed up all our holy reserve some eight months beforehand, so the last [illegible] test expansion was asked for and authorised with the influx of 150 Wrens into the R.R. and the D.F. during the spring of 1944. But more weight of bodies was by no means the [illegible] of our difficulties in these rooms, to whose problems I will return later.

The first essential was to cut the stage cryptographically. It was clear that the Second Front would confront us with far more operational keys than we had ever had before, and it was essential to practice the Watch in dealing with them. Moreover, we knew well from experience that enormous advantages accrue from taking over keys on to an operational basis well in advance of the actual operations, so as to accustom the cryptographers who would have to deal with them to their characteristics. This argument is in no way vitiated by the fact that, under the impact of a shock such as the Normandy Landings, these keys themselves would certainly lose those characteristics and develop new ones. The point was that, if only we could get a grip on some of the main keys beforehand, our knowledge of them might help us to tide over the critical transitional stages and to go on breaking until they developed well-defined new traits. With this double object in view then, we transferred as early as March 3rd one of the main French keys, such as Snowdrop and Jaguar, back to the Watch. At the same time we began to transfer back our key-[illegible] research, while Hanisty continued to recruit and train fresh cryptographic staff from every likely source. As we hoped, our knowledge of the invasion G.A.F. keys proved invaluable on D Day and the weeks following.

With the Army keys, we could not do this in advance. There was practically no traffic on the Western Army, so they had perforce to wait till after D Day. But we had a very strong party working under Douglas Nicoll on these Western keys in Research, and a very good party in R.R.2. We also arranged to make a room available so that the minute the time was ripe we could transfer the whole party on to a fully operational basis as a part of the cryptographic Watch, with the corresponding R.R.2 personnel transferred to R.R.1. With that we had to rest content.

The main task of May was to go round the R.R. and the D.R. and try to bring everything up to concert pitch. What we had to fear there was an explosion of traffic so devastating that it would swamp our existing routines, and we had to decide beforehand what we could afford to scrap (for many cases in the most literal sense, by using the waste-paper basket). The worst bottleneck that suggested itself was in the initial sorting, that is, the sorting to identified keys, by means of a frequency guide, as the traffic came off the conveyor belt. It was obvious that if, as we must expect, we had a flood of traffic and a much higher number of urgent operational keys, intolerable delays would be caused at the initial stage. At the last moment, only just in time for the new routine to be adopted, [illegible] Baker of the Control Room hit on the match-winning device of sorting in a different way, by serial instead of by frequency. This was much more economical and

efficient and time-saving, and just made all the difference between coping and not coping at the crisis. Numerous other improvements and simplifications were made, all with the basic object of getting as much as possible of the operational traffic through as quickly as possible; but none was as drastic or far-reaching as this.

The D.F. was the final goal of all, once more the speedy passage of the operational traffic was our main concern. In this connection I made one point which I had the best instincts of the stalwarts of that room, and which also, I think, was accepted with no enthusiasm by Hut 3. That was the so-called "spotty messages" routine, whereby poor hand work was left on one side in hopes of a better one coming, and if one did were ultimately scrapped. How the skill of the expert decoder lies in this very matter of extracting the last ounce from the filthiest text, and it was entirely against the best traditions that the fullest effort should not be put forth against them: it appeared to put a premium on the slapdash or slovenly workers. Nevertheless, it appeared to me that the overriding necessity of getting as much of the important traffic through as quickly as possible demanded this innovation, and I believe that in the most critical period it fully justified itself. However, it was never popular anywhere, and everybody was very thankful when relaxation of the pressure enabled us to return to our former and better standards.

I do not think that it is boasting to say that all these preparations fully justified themselves, and that D Day for Hut 6 could hardly have gone better than it did. The Watch broke practically all there was to be broken of the enormous volume of operational Air traffic. They lived on the old cribs for a day or two, then they lived on re-encodements until the cribs settled down again, which they did when the Germans had redisposed themselves and recovered from the original disorganisation. The R.R. D.R. and Duddery just and only just managed to cope, the D.R. output rising from 1600 before D Day to a peak of 3000 a fortnight later. Traffic began to appear on the Western Army keys, and the transfer to the Watch and R.R.1 was made within a few days. Both the cryptographic and registration Army parties had to be expanded very rapidly, but they too kept their heads above water. By the time the Battle of France was in full swing, they were producing intelligence worthy of our greatest days. In sum, we had swung more fully than ever before, on to an operational basis, and all the sections concerned stood the strain and did their jobs. Actually the level of traffic fell away as quickly as it rose, which was just as well, because I do not think we could have maintained the peak level for any length of time.

Now for the rest of 1944. First of all, the U.S.A.F. In August came the long-dreaded expansion in the use of Uncle E. It meant a lot more work for the cryptographers and we broke a prodigious number of reflectors from then onwards, but it did us little harm otherwise and output showed a negligible decline. In September, however, a serious slump in the intake of traffic occurred on both Air and Army, a serious difficulty which was trying for everybody. In October we took a further important step in organisation, affecting both the cryptographic and identification sides. It had long been obvious that with the ever narrowing circle around fortress Germany, it would become increasingly difficult to maintain clear-cut distinctions between the various geographical fronts. The areas would get mixed up with each other both for cryptography and identification. This was particularly obvious on the Air side, because of the universal Air key, Red, which was liable to be connected with any other key, and therefore

we tackled the Air side first. Since it was becoming impossible without loss of efficiency to segregate G.A.F. keys into groups, the logical course was to abandon the time-honoured distinction between Watch and Research, to pool the total Air cryptographic resources and to put the whole under one management. There was no need and no intention to treat all the keys as of equal urgency, because we had already, in the Watch, an admirable instrument for taking care of the less urgent or less tractable keys. A similar course was adopted by U.S.S., where the distinction between operational and non-operational keys had long lost any relevance. It was clear that there was no logic in having one body - the Duddery - dealing with the Watch keys and another dealing with non-Watch. The problem of the G.A.F. could only be dealt with satisfactorily as one whole.

These measures met with marked success, particularly in the greater concentration of effort which it was possible to bring upon the Eastern Front group of keys. The Faun/Rosevear combination was now reunited and the months of October and November gave us the completest picture we have ever obtained of the G.A.F. in all sectors.

Now for the Army side. The Western Army party had had its crowded hour during the battle of the Falaise gap and the pursuit across France, which must have made up for any amount of dreary and discouraging waiting. However, the glory departed as suddenly as it came, and with the Germans behind the Siegfried Line they were once more reduced to sitting about and waiting. I spoke optimistically in terms of "Jam to-morrow" and said that the final battle would be fought and prophesied better than I knew; but it is not easy to take long views when you are disconsolately reading a book on fretting, and their morale slumped badly. It was not improved, nor was that of the section as a whole, when the initial success of Rundstedt's offensive in the Ardennes showed that we had been taken off our guard, and suggested either that Ultra was losing its potency or that someone had blundered. Neither was true without qualification or extenuation, but it was difficult to explain without appearing to explain away; and coming as it did on top of the general disillusionment created by over-optimistic pronouncements the shock was considerable.

Nor, in the meantime, was the enemy by any means done with on the security side. Nothing in the fight which he put up in the closing stages was more remarkable than the ability and energy of his security officers, nor the discipline which enabled his operators to carry out new and exceedingly complicated security devices. In November he embarked on the Army side on the long-dreaded system of [illegible] coded callsigns, which meant that our last prop for [illegible] was knocked away. It was at this point that [illegible] achieved its crowning triumph, and so for the matter of that did the [illegible] Army Intercept stations as well. They fought and won that battle almost off their own bat, so that the [illegible] preparations made by ourselves and Sixta proved to be largely unnecessary. They were lucky in that the Germans [illegible] their habitual mistake of taking two bites at a cherry, and introduced the three-daily frequency changing before the old one was working; so they had been given time to accustom themselves to the pattern of frequency changes. Even so, that fortnight is like from an outstanding achievement. It will be seen that as the Germans got better and better at camouflaging everything to do with their wireless system, so the problem was pushed further and further back from

Hut 6, first to Sixta and then to the stations themselves, because it was in the last resort the individual operators who now had to make suggestions based on similarities of procedure and so forth, for the continuity of their own groups. We were more and more in the position, not of doing the sorting and identification job for ourselves, but of so organising ourselves that we could make the most effective and immediate use of the help which we were receiving from outside. That is why I said at the beginning that the role of the earlier members in the chain, the stations and Sixta, became steadily more important.

Not, however, that our own task became any easier. On the contrary, the organisational problem became steadily more complicated. Now it had been clear for some time that in the end we should have to do for the Army what we had done for the Air in October, and for precisely the same reason. One could only do the identification job properly by treating the Army traffic as a whole, with the same group of experts working upon it; and this had already been done in the division of T.I.S. into T.I.S. (Air) and T.I.S. (Army), under a common head. Cryptographically, the high-level general keys tended less and less to confine themselves to one particular Army group or area, while re-encodements from any area or key might provide an entry into any other. Again, therefore, the distinction between operational and non-operational traffic, while still partially valid for intelligence, could no longer be maintained for cryptography. To get the best results for cryptography, it was necessary to bring all the Army cryptographers together; and to get the best results from the cryptographic effort as a whole, it was necessary that the Army and Air sections should be jointly administered, for the policy that dealt with the bombes and with the priorities of keys, not only of Air against Air or Army against Army, but of Air against Army, could only be efficiently directed by one man. Nor, on the basis of divided responsibility, could one have made the best use of the available cryptographic resources, which involved frequent and rapid redisposition of forces between the two sections, in accordance with the changes in the difficulty or importance of various Air and Army keys.

The final act of 1944, then, was to say goodbye with regret to the conception of Research as a separate entity, to put the Army all in one room - the old Research - and to put all the Army registration in the old R.R.2 leaving R.R.1 for the Air. Major Manisty took administrative charge of the Air and Army Watches and Quatches, and Miss Hollington of the two R.R.'s - again for better use of the available personnel, and because so many of the problems of administration were common to both, and could not be settled in one room without reference to affairs in the other. For sentimental reasons the changes were not popular, but I think the critics would even then have admitted that the logical case was conclusive, and that the practical difficulties - space, distance from the operational centre, etc. - could be overcome; and we could feel by the end of 1944 that we had in the long course of the years, not wholly or violently, but by evolution and persuasion, evolved a simple, compact and logical organisation with which to face the final battle.

0·36 1945 : FINALE

The story of 1945 is simple and clear cut. On the Air side it comprised the final battle of February, the longest and hardest of any of our crises, but victoriously surmounted in the end. On the Army side, there was a crescendo of success from February onwards right up to the end, so that though the Air had a record of almost uninterrupted success for five years, the Army with on the whole the much more difficult task had the satisfaction of doing their best and most complete job in theclosing months of the war. The Air were going down hill in April, but bad though Uncle D. was, their difficulties were caused principally by the enemy going down hill still faster.

I was always glad that February 1st happened. It showed that the Germans could do the worst they could think of and still fail to shake off our grip. Once again Davies was the moving spirit behind all the plans which were made, the man who could see the problem as a whole, and who could produce and formulate the constructive ideas to deal with every part of it. But much more than before it was an operation in which everybody played his part, not only once the battle was joined but in all the preparations beforehand. No doubt for that reason and because we had learnt by experience, it was a much better conducted operation than that of April 1st in the previous year. The first few days were extremely tense, but there was never any feeling that matters were getting out of hand. The worst difficulties were those of the cryptographers, and they had some extremely bad days in which they were obviously under great strain and fearing in their own minds the possibility of defeat. I never had any real doubt that they would find the cribs without anything to find them by, and so in the end it proved. The course of events is shown by the drop in our output from 1300 or so in January to 1000 or less, around which level it hovered for the first three weeks of February. Then there was a distinct turn for the better, and the level became stabilised at 12 - 1300. At the end of the month it started to climb steeply again, and by the second week in March we were back again in our full stride. Of course for the rest of the war a lot more traffic got lost in the wash and never correctly identified than ever before, but by and large we could claim to have achieved a pretty complete victory. The new regime meant very much harder work all round particularly, I think, for the stations and for the Control Room. But at the same time it made life very much more interesting, and I think that on balance those departments at least were happier after the change than before. The Germans continued as usual to spoil to a considerable extent the effects of their own ingenuity, for first of all the system of encoding was so complicated that they gave up changing every day and made the same callsign do for three consecutive days - an incalculable saving for us; and secondly, they managed things in such a way that they quite unnecessarily started repeating the same cycle of callsigns over again for various groups, leaving us with no work at all to do except find the repeat. But by the time we were able to take advantage of these mistakes, we had already broken the back of the problem in its most sinister form.

Finally, the end of the Army story. The Western Army party sadly rejoined their colleagues in the old Research quarters, and the Registration party also moved back to R.R.2, now known as R.R. Army. Now because on balance the Army keys had always been the most difficult, and therefore remained in the category of Research (I exclude of course the African and Italian Army

keys), and because they were remote from the bustle and activity of the Air Watch and the N.R. and D.F., those rooms had never developed the same "feel" of operational urgency as the ones nearer the scene of action; the range of doing things in a chain, so that if a piece of paper or a page or a decode gets held up at one link in the chain, it will cause corresponding delays all the way down. Partly to combat this psychological difficulty, but chiefly because it was essential if we were really going to handle Army traffic in bulk on an operational basis, we ordered in November, when these changes were made, a conveyor belt from R.R. Air to R.R. Army and a Terrapin one to carry decoded traffic back. This came into operation in February, and in the nick of time. For from then onwards the traffic increased steeply, and so did the success of the cryptographers and the value of their success. Instead of dissipating their traffic over a wider and wider range of keys, as on the Air Force, the Army in the closing stages concentrated more and more of their high-grade traffic on just a few general keys, such as Falcon, Arrow or Puffin. So the contribution of the Army sections at the end surpassed that of the Air in quality, and rivalled it in bulk; and the Army sections had the satisfaction of becoming every bit as operational as the Air, with the conveyor belt sometimes needing as many as three or four girls to stoke it with decodes on their way over to Hut 3.

So in the first three weeks of March, the last preparatory phase before the crossing of the Rhine and the final battle, we were going as well as we had ever done. April by contrast was rather an anticlimax. The Army went on as strongly as ever and the Air cryptographers were busy enough but the advance of the allied armies overran and destroyed a number of old favourites among our keys. Others simply disintegrated in the general mêlée. Traffic fell off very sharply, and in the lovely April weather there was often nothing to do but sit about and pray that the end would not be long delayed. In the last week or two operations were conducted in an unreal atmosphere against a background of ever more lurid and fantastic melodrama. And so to the first week of May, when the Control Room were taking down messages in clear from the stations and enjoying a bigger thrill from them than they had ever had before. The final message of surrender signed by Jodl for Dönitz and Keitel, sent in the small hours of May 7th, came both to the Control and Registration Rooms, and was known all over the Hut on the night shift. It is worth recording, I think, that my appeal to all rooms that it should not be passed on to the day shift was honoured in full, and that the first news they had was in the public announcement, after lunch, on the German wireless. That seems to me of its kind one of the most remarkable episodes in our history. I don't suppose that a leakage at that stage would have done any great harm, but it would be a pity to spoil the Prime Minister's fun - though in the end the Germans spoilt it for him.

0.37 POSTCRIPT

I am very conscious, on finishing this hasty narrative of Hut 6, of how incomplete the record is: that some big subjects are barely glanced at, and others not at all. Some names crop up in the course of the story, others not at all. This is not to say that the names which do appear are more important to the story than those which do not. There is no reference, for instance, to Frank Birkinshaw of the Central Room; to Mary Wilson, the perpetual head of the W.T. (later W.R., taking on the old and honoured title of the Decoding Room, most of whose original functions it performed to admiration); to Harold Fletcher, to whom more than to any one man the happiness of the staff was due; to Mrs. Manning, M.B.E., who succeeded Gaunt as head of the Duddery, and rivalled any man in her technical ability and standing; to Major Dennis Babbage, O.B.E., the Chief Cryptographer; to Jane Holgate, the invaluable A.D.C.; to Sheila Dunlop who graced three of the most important posts in the Hut and was invariably to be found in the tightest place at the worst time; to Major Bundy and his American contingent, who ought to have a chapter to themselves; to the principal heads of shift in the Air Watch, John Monroe and Howard Smith; and to many others far too numerous to mention by name. All of them played an indispensible part in the story of Hut 6; but Hut 6 was bigger than any of its members and they should, perhaps, remain anonymous.

Hut 6 was fortunate in its birth and more fortunate in the job it had to do; most fortunate of all in that by a series of coincidences and lucky chances, mistakes galore by the enemy mixed with his superb efficiency, it was enabled to do its job to the end. I would like to say something on the personal aspect of this organisation, which was far the most important and which was the main reason why it was to many of its members a unique experience.

First, a small body coming together in a time of desperate urgency is bound together by ties much closer and more intimate than can be found in a larger and more impersonal organisation. It was the common determination of all to strive to preserve something of this atmosphere, however vast and complex the organisation became. It is perhaps too difficult to analyse anything so intangible, but so far as we laid down for ourselves any guiding rules of policy to achieve this aim, they went along these lines. We tried to keep the human and personal element in the forefront the whole time. The biggest mistake we made, the neglect of the W.R. cryptographers in 1941 and 1942, was due to neglect of this factor. We had to remember that, among the girls especially, we had a staff which was doing a job that, in itself and apart from the object of the exercise, was despotately dull routine work, and much more monotonous than girls with an academic background, rightly or wrongly, felt they could expect. Whether we could have done better with a different type of labour is a very big question, on which I shall not enter. At any rate it would have meant an organisation run on quite different lines. The point is that the monotony of the work (I am thinking principally of Registration work) was itself deadening to the mind, and that made it much more difficult to maintain the vivid imagination of the importance and urgency of the enterprise, which was essential if staleness and lassitude were not to mar our efficiency. Because the work could not be done efficiently as a matter of meaningless routine with the

surface, or barely even the surface of the mind, and anybody who did it like that was no good.

An added and very serious difficulty was the violence in the fluctuations of the work. Because of the steadily increasing complexity, the long term curve was always upward, and the policy of continuous expansion was absolutely right. But time and again we had longish periods when there was far too little to do, and nothing is more demoralising than to have a boring job and not enough of it. In that respect the D.R. were lucky, because nearly always they had too much to do. The physical wear and tear were greater, but the psychological problems were less.

How did we try to combat these deadly enemies of staleness and boredom ? First, by sparing no trouble to arrange leave when people wanted it, allowing people to choose their own days-off, to change shifts and so on. I am sure that nobody who had to plan an organisation of the size to which we eventually grew would ever have thought of anything but fixed shifts and fixed days-off, rotating according to a predictable plan: simply because of the immense simplification and saving of labour which such a course would have ensured. Nevertheless I am convinced that the opposite course, to which we stuck throughout, repaid us manifold, not only on humane considerations but in the actual efficiency with which the work was conducted.

Secondly, by information. I would myself have liked to go further in the direction of disseminating "inside information" than was possible if the guiding principle of security was accepted, that nobody should know more of the content of the material than was essential for the proper conduct of the job. I would have liked to interpret this dictum rather more elastically. However, it is not of information of this kind that I am chiefly thinking, but of information about the activities of Hut 6 itself, of the state of the game generally on all fronts, of the whys and wherefores of particular changes of routine, and of the broad objects at which particular changes of organisation were aimed. I think it is impossible to explain too much, or to publish one's explanations too widely; and essential, except for overriding personal reasons, to be frank and to put all the cards on the table; also to put them on the table as simply as possible, so that anybody can understand. The results of this are often disappointing, because only the lively and alert will read what is written, and the amount of personal talk and explanation that one can give is strictly limited. But something percolates, and it is there for anybody who is interested. The more everybody can be encouraged to try to comprehend the overall picture, the better. The Hut 6 organism never became so complicated but that anybody who was so minded could understand in broad outline - which is all that was required - what it was all about.

Thirdly, to go round and talk, or perhaps rather to encourage other people to do the talking and to listen, so as to get the "feel" about what the man in the street is thinking, whether about the work or the war or billet or anything else. One can learn more in this way than by any number of formal interviews. The night shift is the best time for this, for there are fewer people about. It has a more friendly atmosphere than any other and people are more companionable and more talkative. Again, I think one is far more likely to do too little rather than too much in the way of aimless wandering. It is also a good excuse for postponing the duller jobs.

Fourthly, discipline. In the sense of issuing formal orders, this hardly ever existed: orders were nearly always given in the form of requests, and accompanied by explanations. Here again the reasons were partly historical, though I think in any case the system, where it is appropriate at all, is likely to give the best results. When we began, there was in any one Room no hierarchy; the people doing the job were all on the same level. As things became more complicated, it was obviously impossible to maintain this agreeable anarchy; somebody had to be responsible, if administration was to be carried on at all. So the system of heads of shift grew up, an innovation looked at askance in the early days - chiefly because those appointed, particularly in the girls' Rooms, were extremely reluctant to appear to push themselves forward or to assume any kind of authority over their colleagues and friends (on rare occasions they went to the other extreme). So any kind of authority there was, was dependent on leadership and personality and not on any kind of sanctions. In nothing was Hut 6 better served than in the calibre of its heads of shift in all sections. It was they who really ran the Hut and they were the anonymous heroes and heroines of the story. The great thing about them was they were all so keen on the job. They had a genuine sense of responsibility, not in a heavy or pompous fashion, but because they realised how important their job and that of the Hut was, and they retained the same sense of excitement and high adventure which was the essential background of our work. Without that stimulus, I don't know whether it would have been possible to run a section which involved so many comparatively high-powered people doing work that involved so much drudgery, on anything like the lines which we adopted.

I should now like to try and appreciate how far these methods succeeded and where they failed. It was, as I have tried to describe, a very loose and informal organisation with only an indispensible minimum of formal routine meetings. I left heads of departments with a very free hand in their own department and in nine cases out of ten accepted their advice without question; confining myself to making sure that I understood pretty clearly what was going on and to encouragement. They did the same by their head of sub-sections, and heads of sub-sections by heads of shift. Each department would have its own meetings of heads of shifts whenever it felt like it. When major changes threatened, we would all get together at all levels, but avoiding as far as possible the monster general gatherings at which it is almost impossible to get anything done. As far as possible, therefore, each Room took care of itself. But the more complicated matters became, the more closely did the affairs of each department become entangled with the affairs of every other, and our own with other sections such as Sixta, Hut 3 and the stations. In the end we found it necessary to set up special liaison committees between the different departments, not on the top level but on the head of room or head of shift level, to make recommendations to myself and to heads of departments. I think this was a good idea, but the war came to an end before the committees had got fully into their stride. The guiding principle all along was not to lay things down from on high, but to bring everybody into consultation, to get general agreement and to make everybody feel participants and not cogs in an unintelligible machine.

It is easy to enunciate high-sounding abstract ideals of this kind, not easy to carry them out in an organisation of 550 people divided up into at least nine largish groups (Watch Air/Army, R.R. Air/Army, T.I.S. Air/Army, M.R., D.R., Control); and it would be absurd to maintain that we fully carried our intentions into effect. But it is true to say that the only Rooms which caused no

real anxiety over a long period were the two Registration Rooms. That was emphatically not due to any short-comings in those who were charged directly or indirectly with the responsibility of running them, but simply to the fact that they were much the most difficult Rooms to run. To the psychological problems which loomed more largely in that section that any other I have already referred; but there were plenty of other worries. First, the Rooms were used as a reservoir from which the expansion of other sections doing more highly technical work was fed. Sooner or later nearly all the most promising recruits were transferred in this way, so that the turnover was much higher there than elsewhere. Moreover, those who by reason of ability and personality were best fitted to lead were naturally those most sought after elsewhere. The difficulty was to find enough girls of the high calibre required for the very harassing and responsible job of head of shift, who could stand the racket indefinitely and would waive the possibility of promotion to much more interesting work.

Secondly, it was a vast Room - over 30 a shift, far too big for adequate supervision and with far too many different kinds of routine. The complaint was common and had a real foundation, that the routines had to be changed so often and the same girl only came back to the same job at such rare intervals, that she never properly mastered it. The obvious answer to that is specialisation and subdivision, so that one team does certain jobs, e.g. sorting, and another others, e.g. registration. But the objection to that was, that all the jobs were intrinsically so dull, that the only way of keeping even reasonably fresh was to have plenty of change and variety.

Thirdly, the rooms suffered much more from dilution than any other, except the D.R. which was a much easier problem. There was a much longer tail, and however cunningly the head of shift might dispose of her resources, the weaknesses were always liable to let her down. Everything therefore in that section militated against everybody's being on their toes and on top of the job all the time, and this was most noticeable not only in a great deal of needless inaccuracy, but in the speed with which urgent traffic was handled. It was always possible in a short campaign to bring the speed up to the highest possible level. There was no reason why it should not have stayed there, but it never did; as soon as one's foot was removed from the accelerator, the speed began to slip back. I am sure it was lack of imagination, the deadening effect of monotonous routine over a long period. It is one thing to be told that speed means lives, another to realise it. In a smaller room one might have overcome this deadweight of inertia: with the governing conditions what they were, I am convinced that nothing but Prussian methods would have succeeded; and equally clear that we had immeasurably more to lose than to gain by adopting them.

It is easy to criticise the R.K., because standing in the centre of things and serving all other departments, it stood to be shot at, and had nobody to shoot back at. Its mistakes were bound to be observed, and neither its merits nor its difficulties were always fully appreciated. In all the circumstances, I think it did at least as good a job, and perhaps a better, than could reasonably be expected, ever though that job never came anything like as near to 100% efficiency as did those of other rooms. If I were to run Hut 6 again, I would organise the R.R. differently; but I have no idea how. The great thing about the R.R.'s was that you could always rely on them to rise to an occasion. In R.R.Army, if there was more work to do than they could get through they worked over-time till it was done; not once in a while, but for weeks on end,

not as a special spurt, but as a matter of tradition. In R.R. Air, which bore the brunt of nearly all our worst crises, the more hectic things were the better they liked it. Their heads of shift worked two shifts; they were full of good ideas of how to improve the routines; the best girls, including newish ones with no old Hut 6 tradition, worked as though they were 1940 volonteers; and the Room as a whole accepted without complaint the inevitable stoppage of leave. In all this they were not peculiar to Hut 6, but it did them, perhaps, more honour. That they responded in this way, was due, I think, partly to the fact that we tried to treat a staff of 500 in the same way as a staff of 50 - as individuals and not as units.

0·38 F.S. MILNER-BARRY

To round off the sketch of Hut 6 history just given it seems imperative that another pen should estimate the individual nature and the extent of the personal contribution of F.S. Milner-Barry, the second Head of the Hut, to the success and happiness of the whole organisation.

Before October 1943 Milner-Barry, as head of the Crib Room and then of the Watch, had already set his mark on Enigma cryptography. In these years he accomplished his most vital technical achievement, his pioneer work in cribbery; he set the Crib Room on its feet and none ever surpassed him in his flair for picking out the essential message from a miscellaneous mass of traffic or in his skill in manipulating difficult re-encodements. Yet, as time passed, increasing responsibilities of internal organisation and liaison with Hut 3 inevitably debarred him more and more from the technical field; and by his success in these new tasks he stood forth as Welchman's natural successor in October 1943.

In nothing, perhaps, was Hut 6 more fortunate in that the differing talents and capabilities of its successive heads were so admirably adapted to the circumstances of the times in which they assumed their responsibilities. Milner-Barry himself has already well depicted Welchman's peculiar genius; but if his originality of mind, strong mechanical bias and imaginative vision were invaluable assets for one presiding at the birth of an infant organisation and planning its future growth, no less were his successor's administrative and diplomatic talents ideal for controlling and directing the life of an institution grown to adult stature.

By October 1943, indeed, Welchman's main work for Hut 6, the provision of the tools to do the job in the shape of sets, bombes and cryptographers, was virtually done; but in the sphere of organisation many improvements were possible. Hut 6 had expanded from small beginnings in a natural but at times unplanned and haphazard manner (to take one example only, the Quiet Room, which performed a logically separate function, was administratively, as it was historically, a sub-section of Control); and a great part of Milner-Barry's work was dotting i's and crossing t's, tying up loose ends and removing anomalies generally. For a Hut of several hundred members the loose organisation of 1940 was no longer sufficient. At the time of Milner-Barry's assumption of office the higher authorities were requesting each section to prepare a description of its organisation, and the paper on the Organisation of Hut 6 drawn up by Milner-Barry shows clearly his keen interest in this aspect of his new responsibilities: the paper in question was by far the fullest account of the subject yet produced.

But, of course, much had to be done apart from this work of codification. Many changes in organisation proved necessary (whether through German security measures or war developments) and some of these were fundamental. Throughout all these changes Milner-Barry's synoptic vision - his ability to see the Hut 6 picture as a whole - and his foresight found the right path. He was able to see the Hut not only as it was at any given moment but as a dynamic and developing organisation; and by an intelligent appreciation of the probable effect of German moves - and our moves - on the problems presented to Hut 6 he was able to play

the Hut 6 game so that plans were ready for all probable contingencies and yet not so rigidly based as to be incapable of opportunist alteration if the unexpected happened. It was largely owing to this planning for which Milner-Barry was ultimately responsible that Hut 6 was never overtaken by events.

In his execution of changes (as distinct from their conception) Milner-Barry showed a rare combination of firm resolve and diplomatic finesse. Except in urgent emergencies, all proposed changes were thoroughly discussed with all parties affected, and the protests of outraged conservatives were patiently heard. While Milner-Barry was rarely, if ever, deflected from a course he had decided on, he was thus able to secure his way in such a manner that even opponents of the solution adopted felt their case had been fully considered. This ensured at least a moderately cheerful acquiescence, the more readily forthcoming as experience continually vindicated the soundness of Milner-Barry's judgment.

Still another important element in Milner-Barry's success was that while constantly endeavouring to systematise the organisation of the Hut he never fell a victim to an unbridled craving for schematic perfection. He never, as his own final remarks show clearly, ignored the human element. So to the end there were some anomalies in the Hut 6 "constitution" which to the last was alive and flexible, never rigid and fixed. It is easy to conceive that others - the Germans, for instance - might have planned a Hut 6 (quite possibly very efficient in its Prussian way) run on very different lines, an organisation more logically administered where the chain of subordination would be more precisely defined; but in such an organisation the true flame of Hut 6; the spirit of free enquiry and camaraderie, would have flickered and died. Milner-Barry gave the Hut the more definite shape it needed without sacrificing its soul; his successful preservation in a Hut of some 500 persons of the spirit that animated the original nucleus of some 50 was not the least of his achievements.

BOOK 1

CRYPTOGRAPHY

"I don't believe there's an atom of meaning in it", said Alice.

"If there's no meaning in it," said the King, "that saves a world of trouble, you know, as we needn't try to find any. And yet I don't know," he went on, spreading out the verses on his knee, and looking at them with one eye; "I seem to see some meaning in them, after all."

CHAPTER 1.0

THE GERMAN ENIGMA MACHINE

1.0 PREFACE

The German Enigma Machine is a mechanical device for performing a varying simple substitution on the consecutive letters of clear text.

1.1 DESCRIPTION

The machine is contained in a wooden box about a foot square and six inches deep. It consists of three WHEELS (Walzen) mounted between the CURRENT ENTRY DISC (Eintrittswalze) and the REFLECTOR (Umkehrwalze), together with a KEYBOARD (Tastenbrett), LAMPBOARD (Lampenbrett), STECKER BOARD (Steckerbrett), BATTERY, and SWITCH (See Diagram 1). The lid of the box contains spare lamps, plugs, etc., and the whole is fitted with a handle for carrying.

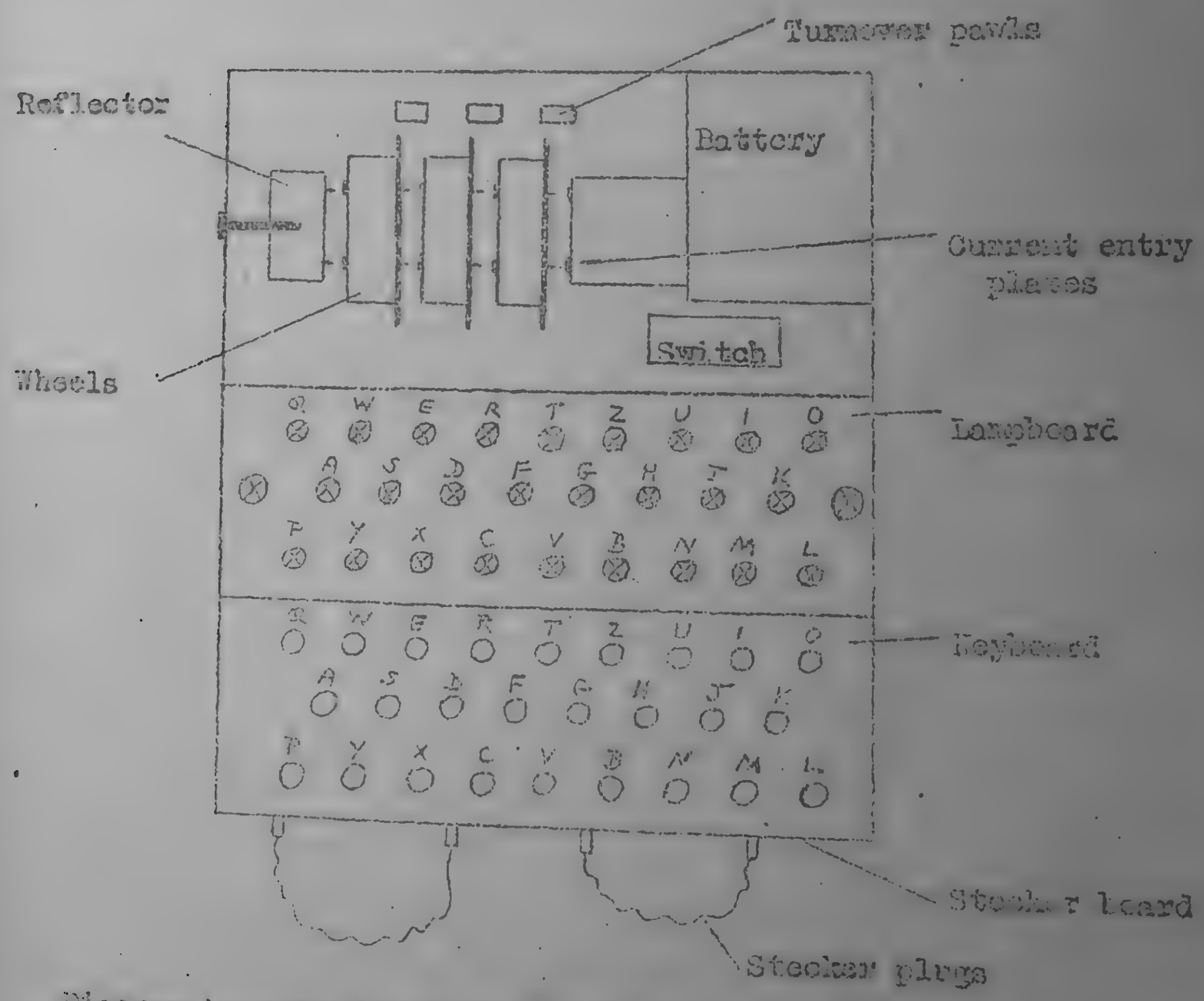


Diagram 1 -- The Layout of the German Enigma Machine

The current entry disc is a ring of 26 terminals (the CURRENT ENTRY PLATES), and these are connected in alphabetical order - via the steeker board - to the key and lamp contacts (See Diagram 2 in the Appendix).

Each wheel has on one side 26 pin terminals, and on the other 26 plate terminals. The 26 pins are connected to the 26 plates in a batted order. On the right hand side of the wheel (as it stands in the machine) is a toothed cogwheel; on the left hand side is a metal TYRE (Ring), marked with the numbers 1 to 26 in order, settable in any position by means of a clip, and provided with a TURNOVER NOTCH on its extreme left hand edge. There are five wheels, all differently wired. The notches are in different tyre positions on each wheel. (The Naval Enigma Machine has three further wheels - VI, VII, and VIII. Each of these has two turnover notches - at points diagonally opposite each other on the tyre - and the notch positions are the same on each of the three wheels.) Any three wheels, in any order, may be in the machine at a given time.

The reflector is a ring of 26 pin terminals which are connected together in pairs. (Normally the "B" reflector was used. Latterly, however, a pluggable one - "D" - was introduced on G.A.F. keys, and a few Army keys.)

When wheels are in the machine the 26 current entry plates are connected together in pairs by electrical paths through the wheels, the reflector, and back again through the wheels. The actual connections depend, of course, on the wheels involved and their positions. (Wheel positions are read off from windows on the cover of the machine.) The pressing of a key sends current through the steeker connections into the machine. The current emerges at the contact of another key, and the corresponding lamp lights up (See Diagram 2).

The steeker board has two sockets corresponding to each letter. These are made to take 2-pin double-ended STEEKER PLUGS (the pins are of different sizes to prevent accidental inversion). When the steeker board is not plugged the connections between the current entry plates and the key and lamp contacts are straight - viz. A to A, B to B, C to C, etc. The insertion of a steeker plug between, say, I and V is equivalent to interchanging these letters on both keyboard and lampboard (See Diagram 2).

Every time a key is pressed one or more of the wheels turns over - thus altering the substitution. This motion is controlled by three TURNOVER PAWLS at the back of the machine which engage with the ratchets and turnover notches. The effect is as follows. The right hand wheel turns over once each position, irrespective of the motions of the other wheels. The middle wheel turns over whenever the right hand wheel is in a "turnover position". The left hand wheel and the middle wheel turn over whenever the middle wheel is in a "turnover position". This last type of turnover is called a "double turnover" or (quite illogically) a "middle wheel turnover". (A wheel is said to be in a "turnover position" when a notch on its tyre is ready to engage its appropriate pawl. The window readings in such positions - called TURNOVER POINTS - are as follows:- Wheel I - Q; Wheel II - E; Wheel III - V; Wheel IV - J; Wheel V - Z; Wheels VI, VII and VIII - M and Z.)

TO BE FILLED IN USE

The "machine setting" consists of:

(i) Wheelorder: three wheels in a definite order, read from left to right.

(ii) Ringstellung: tyre settings on the three wheels, also read from left to right.

(iii) Steckor: the cross-plugging on the steckor board, usually ten pairs, involving twenty letters. (The remaining six letters are unaltered.)

(iv) Reflector plugging: when the pluggable "D" reflector is used.

To encode a message, the three wheels are set at certain positions - called the "message setting" - and the keys corresponding to the letters of clear text are pressed successively. The lamps which light up give the letters of the encode. The turnover(s) actually occur before current enters the machine, so that the pairing "clear text-encode" refers to the position immediately following the position actually set up. Also, from Diagram 2, it is clear that the relation between clear text and encode is reciprocal - a fact which makes encoding and decoding exactly similar processes.

It should be noted that the machine gives a substitution only of the letters of the alphabet to each other. Alphabetical conventions must therefore be adopted for figures, punctuation marks, brackets, etc. Also, because of the way the machine is constructed, no letter can encode into itself.

FOUR-WHEEL MACHINE

The Naval 4-wheel machine is exactly similar to the above except that the reflector is replaced by a "reflector plus wheel" combination. The wheel is, of course, on the right of the combination; it may be set at any position, but does not move during encoding. The reflector is thinner than the normal one, but mounted in the same way. The wheel may be either 'Beta' or 'Gamma'; the reflector either 'Bruno' or 'Caesar'.

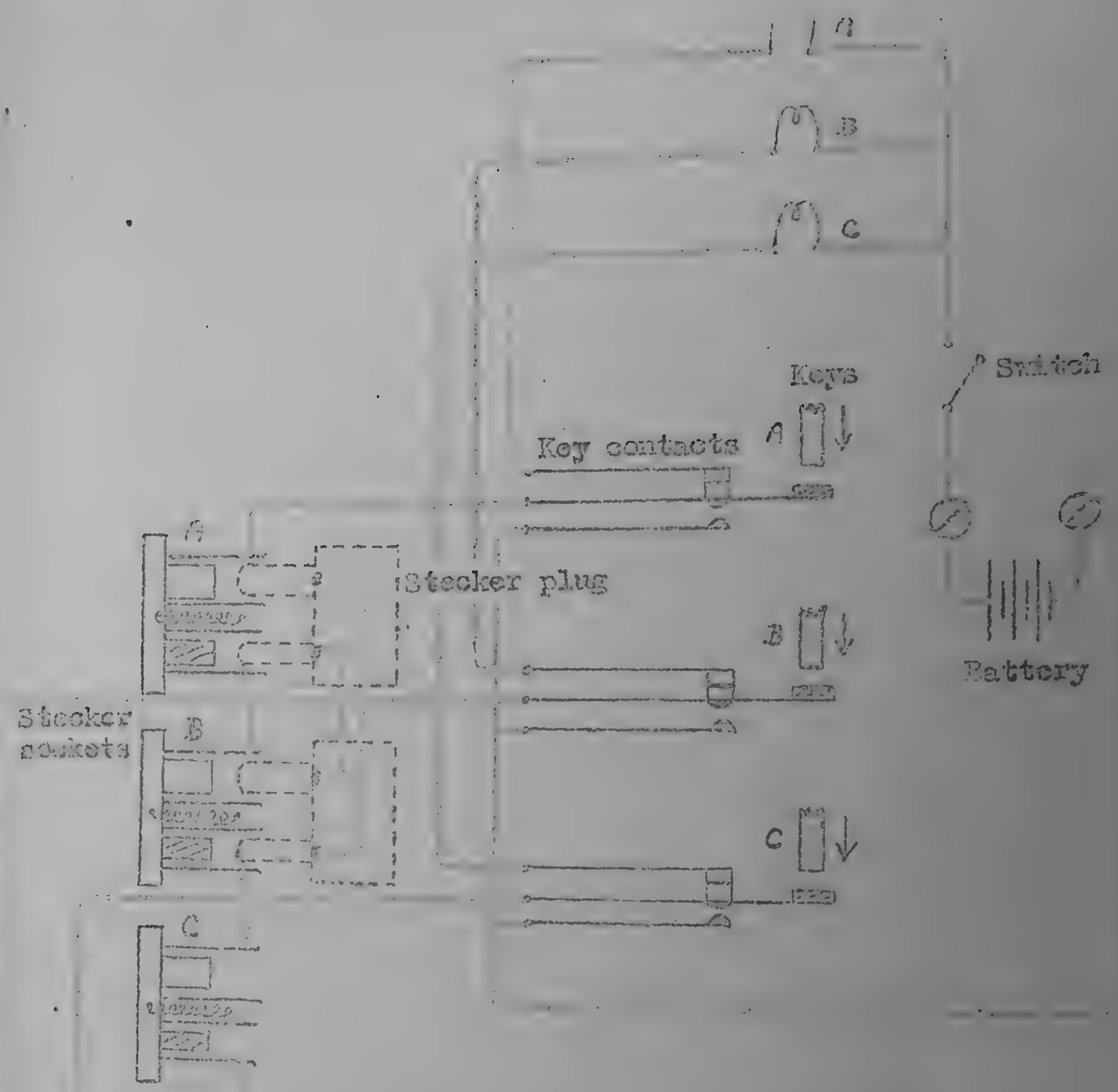


Diagram 2 - The Wiring of the German Enigma Machine

CHAPTER 1.1

PERIOD I : PRE-WAR AND SEPTEMBER 1939 - JANUARY 1940 :

THE BEGINNINGS

1.10 INTRODUCTORY

Although Hut 6 did not exist as a building and can hardly be said to have existed as an organisation before January 1940, the nucleus of its original members was assembled at the beginning of the war. As early as October 1939 there was a fairly full knowledge of the cryptographic problem as it then was, and work was already in hand on the devising of methods and apparatus for its solution. All this knowledge, however, was based on pre-war information. We could not be certain that the enemy had not modified the Enigma machine in readiness for the outbreak of war, and we did in fact have information that he had done so; it was not until January 1940 that this particular fear was set at rest by the breaking of a war-time key.

In the late summer of 1939 we received vital information about the Enigma from the Polish cryptographers, culminating in the reconstructed machine which they presented to us in October 1939. Without this the work of Hut 6 would have been postponed for many months; for although advances might have been made in the theory, we could have taken no practical steps before capturing a machine, which we did not do before the Norway campaign; certainly we did not on our own account collect anything like sufficient data for breaking the machine before then. As it was, this first capture came rather as an embarrassment than otherwise, lest the enemy should as a result introduce new wheels or other security devices; it was in fact shortly followed by a great improvement in the indicating system, but it is doubtful whether this was a case of cause and effect, rather than a step that was bound to be taken as soon as the enemy realised the weaknesses inherent in the old system.

Although routine breaking did not begin before 1940, there is no doubt that the real dividing line between groping theory and operational practice coincides with the arrival in this country of the information from Poland. This event would make a suitable starting-point for our history, but a brief summary of the earlier work in this country and in Poland will add to the completeness of the picture that we shall try to present.

1.11 PRE-WAR : EARLY THEORY

1.110 The First Crib

Machines of the Enigma type had been familiar to us for several years. An unsteckered version, the Commercial Enigma, was on the open market, and a similar machine, with three wheels and no stecker, had been used by the Germans during their intervention in the Spanish Civil War and solved by Knox. Some time before the war (the provenance and date are unknown to the writer, but the latter was certainly prior to February 1939) there had come into our possession a clear-text, its Enigma equivalent, and the key with which the encipherment had been performed. This key contained stecker and provided our first information of this additional complication. The crib was attacked without success by various people at different times throughout the first six months of 1939. The stecker had merely the effect of imposing a substitution on the clear text letters entering the machine and the inverse substitution on the enciphered letters emerging. With the stecker known in this case the effect of this substitution could be stripped off, so that we had

effectively a crib on the unstecker ed machine.

1.411 Pods and Wheel-breaking

The method of recovering the wiring of an unsteckered machine from a crib was sufficiently well- nown, though it was later to be given greater precision; it had been used with success by Knox in his solution of the earlier machine. The theory is too complicated for detailed exposition here (a full account is given in the first part of the technical volume) but some of the basic notions involved may be briefly indicated. Most important of them is the idea of a "rod". Suppose we have an Enigma wheel with known wiring. We denote the positions of the 26 left-hand terminals of the wheel consecutively by a, b, ...z and those of the right-hand terminals directly opposite them by A, B, ...Z (Left and right here apply to the wheel as it would be looked at when in position in the machine though here we are considering the wheel in itself with no reference to the rest of the machine; note that a, b, ...z, A, B, ...Z are attached to the positions of the terminals, that is actual fixed points in space, and not to the terminals themselves. Suppose the wheel is in a position which we may call, arbitrarily, position 1. At this position the point a is joined by an internal wire of the wheel, to, say, the point T. Now let the wheel rotate (in the direction z, y, x, ...) into position 2. A different wire now joins a to, say, Z. Proceeding thus we obtain a sequence of 26 letters, say T Z E Y L X M W I V K U J A L S I R F Q C Q V N Q N, which we call the "a rod". Similarly we obtain the rods of b, c, ...z, the wheel starting position being the same in every case. Note that the 26 letters of the a rod in this example are not all different. Like letters arise from parallel wires; of the 26 cross-wires of a wheel at least two must be parallel, so that a rod necessarily contains at least two letters the same.[X]

Each rod clearly contains in itself full particulars of the wiring and the rods are not therefore independent. The connection between them is easily seen. Suppose at a certain wheel position a particular wire joins, say, q to R. When the wheel moves one step (in the direction z, y, x...) this same wire will now join p to R. Thus if a letter occurs at a certain position on a given rod, the next letter in the alphabet occurs at the preceding position on the rod next in the sequence a, b, ...z. This "diagonal property" enables us to write down all the other rods given the a rod, and we thus obtain the "rod square":-

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
a	T	Z	E	Y	L	X	M	W	I	V	K	U	J	A	L	S	I	R	F	Q	C	Q	V	N	Q	N
b	A	F	Z	M	Y	N	X	J	W	L	V	K	B	M	T	J	S	G	R	D	R	W	O	R	O	U
c	G	A	N	Z	O	Y	K	X	M	W	L	C	N	U	K	T	H	S	E	S	X	P	S	P	V	B
	-	-	-	-	-	-	-	N	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Q	-	-	-
	-	-	-	-	-	-	O	-	-	-	-	-	-	-	-	-	-	-	-	-	-	R	-	-	-	-
	-	-	-	-	-	P	-	-	-	-	-	-	-	-	-	-	-	-	-	-	S	-	-	-	-	-
	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
	-																									
	-																									
	-																									
a	H	S	Y	D	X	K	W	L	V	H	U	J	T	I	Z	K	R	H	Q	E	P	B	P	U	M	P

[X] This is true of an Enigma-type wheel with an even number of terminals; it is not necessarily the case if the number of terminals is odd.

The column 1(the particular choice of column is of course arbitrary) is known as the "wheel upright".

Consider now the wheel in position in the machine at the right-hand side. We can identify the points A, B, ...Z with the terminals of the entry plate(Eintrittswalze). Suppose now we have a plain text and its cipher equivalent. Each constatation of this implies a pairing of two of the points A, B, ...Z by electrical connections through the three wheels and reflector and back again. If the starting position of the right-hand wheel is known or assumed this pairing implies a pairing of two of the points a, b, ...z, say a and b by electrical connections through the two left-hand wheels and reflector and back again. So long as the two left-hand wheels do not move,that is in general for a stretch of 26 successive positions of the right=hand wheel,this pairing of the points a, b or ab rod pairing, will persist. There will be for the stretch 13 such fixed pairings,which may be regarded as the pairings of the composite reflector formed by the reflector proper and the two "fixed" left-hand wheels. Thus among the 26 rod pairings determined by the successive constatations in the stretch of crib there will be several which occur more than once. It is from these considerations that we can, given a crib, attempt to recover the wheel uprights (and therefore the wiring)of an unknown wheel.

It is necessary to assume the positions(at intervals of 26) when the middle wheel turns over. With a long crib it may not be necessary to make all 26 assumptions in turn;we can assume that the turnovers come in certain stretches, say of 5 or 6 positions, at intervals of 26 and confine our attention to the remaining stretches; we can in this way cover all possibilities with five or six different assumptions of turnover areas. Since the wheel wiring is unknown we can with no loss of generality assume that the right-hand wheel is in position 1 for the first constatation of the crib.

Consider now two consecutive constatations within a non-turnover stretch,say at right-hand wheel positions 8 and 9. Provided,and this is a most important point,that we know the wiring of the machine from keyboard and lampboard to the(double)terminals of the Eintrittswalze, these constatations can be translated into pairings of the points A, B, ...,Z; let us say W/X and I/M. Now it may be the case that the wire of the right-hand wheel which is opposite W in the eighth position and that opposite I in the ninth both lead to the same fixed point on the left-hand side, or, in other words, that W and I are the eighth and ninth letters of a particular rod. If this is so then X and M are necessarily the eighth and ninth letters of another rod, the two rods being paired through the "fixed" left-hand position of the machine. Because of the diagonal property of the rod square this hypothesis and its consequence can be translated into properties of the wheel upright and we may say that if D is immediately above Q on the upright then E is immediately above U. We may alternatively assume that W and M, and therefore also X and I, are consecutive on a rod; in this case we can say that, if D is next above Q on the upright, E is next above U. Every pair of consecutive constatations within a non-turnover stretch gives us similar pairs of hypotheses and consequences about consecutive letters of the upright. By taking constatations 2, 3, 4... apart we get similar hypotheses and consequences about letters at these distances apart on the upright. It is clear that all these hypotheses and consequences (one which gives the same consequence several times)and to follow

out the chain of consequences until either a contradiction is reached or the upright is filled in. It may of course be necessary to make subsidiary hypotheses from time to time. In case of failure we must proceed to a new hypothesis for the positions where the middle wheel turns over. Once the right-hand wheel is determined we can take all the crib pairings through it and translate them thus into pairings through the two wheel Enigma constituted by the reflector and the two left-hand wheels. A similar process is then employed to recover the wiring of the middle wheel and finally those of the left-hand wheel and the reflector itself.

In the preceding account we have associated the letters A, B, ...Z with consecutive terminals of the Eintrittswalze. It was customary, however, when this was known, to name the terminals by the keyboard and lampboard letters to which they were connected. For the machines with which we were familiar the terminals were connected to the keys(and lamps)in the order in which these appeared on the machine, the "type-writer" order
Q W E R T Z U I O A S D F G H J K P Y X C V B N M L. The fixed points opposite these terminals on the left-hand side of the right-hand wheel were named by the corresponding small letters. When the rods q, w, e, r, ... were written out under each other they would thus form a rod square with diagonal Q W E R .. This convention had the convenience that a clear-cipher equivalence through the unstecckered machine could be translated at once from the rod square into a rod pairing. The rod square diagonal was known as "the diagonal of the machine".

The process of wheel-breaking which we have sketched presupposes the knowledge of the diagonal. Without this knowledge the problem is much more difficult and it requires either a very long crib, about 2000 letters, or a very specialised one, as for example a knowledge of all the 13 pairings through the machine at each of nine consecutive positions together with two pairings at a tenth position. Information was not at our disposal, and it was therefore necessary to guess the diagonal. The obvious guess was Q W E R T Z U - - - - L, when this failed, this order was tried in reverse with equal lack of success. The correct diagonal, which is in fact simply A B C D ..., was either not tried or, if it was, and the evidence is conflicting on this point, the attack was not pressed home. When, months later, we had definite knowledge of the diagonal, the crib was again attacked and the wheel wiring successfully determined; but by then the problem was an academic one.

It fell out very quickly then (Twinn)

It is difficult not to feel that the alphabetical diagonal should have been considered earlier, but it must be remembered that, from a constructional point of view, it is a most improbable one. In the various Enigma-type machines in which the security depended on multiplicity of turnovers the diagonal adopted was always the constructionally obvious Q W E R T Z U ... It is difficult to see why the Germans should have adopted a different practice in this case, especially since their notion of stecker gave what was in effect a device for the arbitrary hatting of the diagonal. The only argument in favour of the alphabetical diagonal would seem to be that it is a rather more convenient one for a theoretical study; but this is a very small point. The unfortunate fact remains that the diagonal was not guessed and the breaking of Enigma was thereby probably postponed for six months.

In addition to the attack on this crib there was being examined in the spring and early summer of 1939 traffic bearing all the characteristics of encipherment with the Enigma. The most obvious characteristic, common to all machine encipherments, was the flat distribution of letters; but what made the use of the Enigma particularly certain was the indicating system employed. The system that was being employed in early 1939 continued right through to the end of April 1940. This system will be described later. Most of the research work that was being done in the spring of 1939 was on traffic of earlier years which, while in clear continuity with current traffic, employed a primitive and most revealing system of indicating.

1.112 The Indicating System and its Vulnerability

Traffic on one key could be identified by its Kenngruppen or discriminants. A discriminant consisted of a group of three letters and each key had four discriminants. The first five letter group of an Enigma message consisted of two dummy letters followed by a discriminant group, whose three letters could be in any order: on a few occasions the dummy letters occurred at the end of the first group. The linking together of the four discriminants used by a key could usually be done from an examination of the first groups of a message with several parts. (At a considerably later stage the use of different discriminants for the different teile of a multi-teile message was forbidden.) When several messages on the same key were written out under each other a certain set of six consecutive letters at the same position in each message was seen to have significant characteristics. This was the indicator group. Its position varied from time to time but was fixed for a particular key: it was always near the beginning of the message and started at the boginning of a five letter group. A number of such indicator groups, written under each other might present the following appearance:

A M V B L S
C T U K Z C
A R K B R Z
C T K K Z Z
D O C E Q V
D T V E Z S
. . . . . .
. . . . . .

It will be seen that each occurrence of A in the first column is followed by B in the fourth, similarly D in the first is followed by E in the fourth, T in the second by Z in the fifth, and V, K in the third by S, Z respectively in the sixth. Generally the occurrence of a letter in column n($n = 1, 2, 3$) implied the occurrence of a definite associated letter in column $n + 3$. This phenomenon makes the indicating system fairly obvious. Part of the key consists of a Grundstellung, or basic setting of the three wheels. Each message is enciphered at a message setting (or inside indicator) at the choice of the operator. In order to disguise this setting, which must be conveyed to the recipient in order that he may decipher the message, it is enciphered twice at the Grundstellung, and the resulting six letters sent as indicator group. The recipient sets up his wheels at the Grundstellung and deciphers the indicator group, obtaining the result, say, X Y Z X Y Z; the message setting is thus X Y Z. This double-encipherment of the message setting is a good check against faulty encipherment or transmission but it has a

fatal weakness,as the sequel will show.

Given a sufficient number of indicator groups of the preceding type it is possible,with a certain amount of inspired guess-work, to read them all,and this with no prior knowledge of the wheel wiring or stecker(if any); this feat was frequently performed. A detailed account of the technique occurs elsewhere,but the method can be lightly sketched here. The explanation is simpler if we start the wrong way round,assuming the solution known. At any position the machine imposes a reciprocal transformation on the letters of the alphabet. This transformation,consisting of thirteen letter-pairings,was known loosely as the "alphabet"at the particular position. Let us call the six machine positions immediately following the Grundstellung positions 1, 2, 3, 4, 5, 6. Suppose the alphabet at position 1 is
(AM) (BZ) (CQ) (DX) (EL) (FG) (HK) (IJ) (NY) (OP) (RU) (ST) (VW)
and the alphabet at position 4 is
(AL) (BI) (CE) (HR) (FX) (GH) (IN) (JS) (MT) (NV) (OZ) (PW) (QU).
Suppose now that A is the first letter of an indicator group. A is the result of enciphering M. Therefore the message setting begins with M. When M is enciphered at position 4 we get V: therefore V is the fourth letter of the indicator group. Similarly B in the first place implies O in the fourth. We give the complete list of consequences:-

Column 1	Column 4
A	V
B	O
C	U
D	F
E	A
F	H
G	X
H	T
I	S
J	N
K	G
L	C
M	L
N	B
O	W
P	Z
Q	E
R	K
S	J
T	D
U	P
V	M
W	R
X	I
Y	Y
Z	

A more compendious notation can be used for this table of consequences. We have A in column 1 implies V in col.4 : V in col.1 implies P in col.4: P in col.1 implies Z in col.4, and so on. This can be expressed in the form
(A V P Z Y I S K G X R Q E) (B O W M L C U D F H T J N)

These are two distinct cycles of 13 letters, both EA and NB being regarded as consecutive. If two letters are consecutive in either cycle then the occurrence of the first in position 1 of the indicator group implies the occurrence of the second in position 4. We call the above expression the "box" of indicator columns 1 and 4.

We now "box together" the alphabets at positions 1 and 4; that is we take any letter, say A, and write after it its pair in alphabet 1, in this case M: after M we write its pair in alphabet 4, which is V: after V its pair, W, in alphabet 1, and so on. The final result is

(A M V W P O Z B Y N I J S T K H G F X D R U Q C E L),

a cycle of all 26 letters.

If we take alternate letters of this cycle starting with A we get A V P Z Y I S K G X R Q E, and starting with M we get M W O B N J T H F D U C L. The first of these is one of the 13-cycles of the indicator column box; the second is the other 13-cycle written backwards.

Consider now the problem as it would be presented. Given enough indicator groups we should have the data to form the box of two 13-cycles of indicator columns 1 and 4. There are 13 different ways in which the letters of the second cycle written backwards can be inserted between alternate letters of the first. We thus obtain 13 possible 26-cycles for the box of alphabets of 1 and 4. Each is a possible solution, the alphabets being read off direct from the box.

In this example the indicator column box consists of two 13-cycles and the alphabet box of one 26-cycle, but this will not happen in every case; there may be a larger number of smaller cycles. What we can say, however, as a little consideration will show, is that for every cycle of length m seen in the indicator column box there must be another cycle of the same length, the two combining to form a 2m cycle of the alphabet box. Given the complete box of two indicator columns we can always find a finite number (12 or more) of pairs of alphabets at the corresponding positions. Hence, boxing similarly columns 2 and 5 and columns 3 and 6 we deduce 12^3 or more possible sets of alphabets at the six positions. Any such solution will decipher each indicator group in the form XYZXYZ.

In theory any one of these solutions is as good as another, but in practice this is not so. This is because the message settings, being at the operators' free choice, tended not to be perfectly random. In particular, it was unlikely for a message setting to contain a repeated letter, and any solution giving a lot of such settings could be rejected. The most powerful criterion at that time was "the middle vowel". It was assumed that pronounceable trigrams would be popular as settings, and therefore any of the 13 or so possible solutions of the 2,5 alphabet box which gave a large count of vowels for the second letter of the setting would have a good chance of being correct. If such a solution stood out convincingly it reduced the possibilities by a factor of 13. It was usually found that among the sets of settings produced by the different solutions of the other alphabet boxes one was clearly better than the rest, as containing such likely pronounceables as GUT, WAL, FRO, etc., and keyboards like ASD, WIL, REV, OKL, etc. Such choices were very much commoner in the early days, and there was rarely any doubt about the correctness of the solution found.

1.113 Depth and Turnover

Once the message settings had been determined for a day's traffic it became possible to locate, at least approximately, the positions of the turnover notches on the middle and right-hand wheels. This was done by "setting messages in depth". If two plain language texts are written out one under the other and the "clicks"(occurrences of the same letters at the same place in each) are counted, there will in general, because of the irregular distribution of letters in language, be more than one click for every twenty-six letters, which is the random expectation of two texts consisting of arbitrary jumbles of letters; there is also the chance of a repeat of several consecutive letters arising from a common word or syllable. This high "repeat rate",which varies with the nature of the plain text but which was in the neighbourhood of one in 17 in the kind of German plain texts that we met with, will clearly persist if the two texts concerned are both enciphered at the same position of the machine. Texts enciphered at different positions have a random repeat rate when counted level. Suppose now we have two messages whose settings have been determined as GUN and GUT. If the right-hand wheel has a single turnover at one of the positions N to S inclusive, the second message will be enciphered with a starting position 20 preceding that of the first: if the turnover is at one of the positions T to M inclusive then the starting point of the second message will be after that of the first. If the hypothesis of a single turnover is right the correct alternative can be determined by staggering the messages appropriately and counting the repeats; in one case the count will be flat and in the other that of plain language. Similarly we may be able to limit the possible turnover positions of the middle wheel. Thus two messages with settings DER. EER may have a convincing level count,perhaps with a long initial repeat. This suggests that the middle wheel has turnover position E, so that EFS is the wheel-reading immediately following each of the above settings.

By methods of this sort the existence had been established of three wheels with turnover positions Q, E and V, the wheelorder varying from day to day. These turnover positions were actual window-readings of the wheels,so that the turnover notches were necessarily on the tyre and not on the main body of each wheel,as had been the case with some types of machine we had seen.

The knowledge on any particular day of the alphabets at the six positions following the Grundstellung was not in itself sufficient for the discovery of the wheel wiring. To obtain further evidence attempts were made to get cribs by "reading messages in depth". With the wheelorder and message settings known for a day's traffic,all messages could be set at their correct relative positions and numbers of depths or overlaps obtained of parts of messages enciphered at the same position. The theory of reading such depths is simple enough but the practice is difficult in the extreme. Suppose we have four Enigma texts in depth:-

. . . . T P N E V H Z . . .
. . . . X P N E V H T . . .
. . . . Y P I S Q L C . . .
. . . . R P M N D O A . . .

The letter P occurring at the same position in each text is likely to be the encipherment of a common letter such as E. If this is so it suggests the possibility that the clear text of PNNV,common to

the first two messages, is the common tetragram EINS. On this hypothesis we can, because of the reciprocal property of the machine, read additional letters of the last two messages. We have clear text

. . . . E I N S . . .
. . . . E I N S . . .
. . . . E N . . . . .
. . . . E . E . . . .

This looks promising and can be made the basis of further hypotheses. With no prior knowledge of message contents, however, reading in depth is an unrewarding pastime. Even with a reciprocal machine like the Enigma it is doubtful whether anything but a few isolated fragments can be read in general on a depth of less than twenty, and such depths were unobtainable with the small volume of traffic at our disposal, and no effective progress was made on these lines. (In the years to come many ingenious feats of depth-reading were performed, but always with strong presumptive evidence for the probable clear text of one or more of the messages).

1.114 New Wheels and Indicating System: The Goal-hunt

The use of three wheels, giving six possible wheelorders appears to have continued on German Army and Air Force keys until the end of 1938, when two extra wheels, giving a choice of sixty wheelorders, were introduced. Roughly contemporaneous was the change in indicating system. The first group as before contained the discriminant but the characteristic effects of a fixed Grundstellung disappeared, and instead each message had a three-letter group in the preamble. It was an obvious guess that each message now had its own individual Grundstellung, represented by this trigram, for the encipherment of its (repeated) setting. This hypothesis was soon verified and the position of the indicator group determined by writing under each other the texts of messages with the same trigram preamble (or "outside indicator") and looking for repeats three apart. The indicator group was found to be consistently in positions 6 to 11, immediately following the five letter dummy and discriminant group. Thus we might have the following pairs:-

	Outside Indicator	Letters 6 - 11
(i)	A M V	S T Z U K N
	A M V	L T A M K Q
		E E

Here the repeat of T is followed by a repeat of K three places on. Evidence was also obtainable from pairs of messages whose outside indicators were one or two apart. Thus:-

	Outside Indicator	Letters 6 - 11
(ii)	A X T	L A C M Z R
	A X U	A D V Z E K
		Z Z
(iii)	A E C	M V U X L Q
	B F D	V L S L U A
		Z Z

	Outside Indicator	Letters 6 - 11
(iv)	A L Q A M S	N S T Z U B T V Q D X C M
(v)	A D Q B F S	N Z T X L V T C Q V A D M

(ii)is a straight verification of the hypothesis, (iii)is a verification only on the further hypothesis that the middle wheel has E/F turnover,so that the second letter of the first inside indicator and the first letter of the second are both enciphered at the same position EEE(and there again three places on).Similarly (iv) suggests(but does not prove)that the right-hand wheel has Q/R turnover,and (v) that the middle and right-hand wheels have respective turnovers E/F, Q/R.

Evidence of this kind established first the position of the indicator group and then the existence of two wheels with turnovers J/K and Z/A in addition to the three with the turnovers Q/R,E/F,V/W which were already known. The examination for "clicks three apart" of the appropriately staggered indicator groups of messages with adjacent outside indicators was known as the goal-hunt. More important than the clicks or goals that were scored were those that were not. Thus (iv) above only suggests that the right-hand wheel is that with Q/R turnover; but, if the pair had been

A L Q	N S T Z U B
A M S	T V Q D X C M

the fact that T is <u>not</u> followed by a click three places on proves that the right-hand wheel cannot have Q/R turnover.

The new indicating system,lamentably bad though it proved to be when we knew the wiring,came as a serious set-back to the attack on the uncompromised machine. Since it was no longer possible to break the indicators,the chance of a depth crib became still more remote; few depths were discovered,let alone read.

1.115 News From Poland

The preceding pages roughly indicate the lines of attack in the first six months of 1939. Within another month the whole position had been radically changed. At the end of July Knox went to Poland and met the cryptographers there; he returned with the startling news that the Poles had, with varying success, been reading Enigma for several years.

It is historically uncertain how the Poles obtained the wiring of the wheels and machine, and it was not a subject on which they were very communicative. Certainly they made extensive use of secret agents and it is most probable that they obtained photographs of keys and messages with clear-text. The essential fact that the machine diagonal was alphabetical they admitted to have discovered through one agent,though they claimed, no doubt with justice, that "nous avions pu/trouver par mathématique". However much the Poles had depended on agents for their basic information there is no question that they were highly talented men, and that, with limited resources, they had performed brilliant work. In the course of the

	Outside Indicator	Letters 6 - 11
(iv)	A L Q A M S	M S T Z U B T V Q B X C K M
(v)	A D Q B F S	P Z Y X L V Y C Q V A D K E

(ii)is a straight verification of the hypothesis. (iii)is a verification only on the further hypothesis that the middle wheel has E/F turnover,so that the second letter of the first inside indicator and the first letter of the second are both enciphered at the same position BFE(and there again three places on).Similarly (iv) suggests(but does not prove)that the right-hand wheel has Q/R turnover,and (v) that the middle and right-hand wheels have respective turnovers E/F, Q/R.

Evidence of this kind established first the position of the tor group and then the existence of two wheels with turnovers Z/A in addition to the three with the turnovers Q/R,E/F,V/W e already known. The examination for "clicks three apart" appropriately staggered indicator groups of messages with

The statement that the Poles learnt through an agent 'the essential fact that the machine diagonal was alphabetical' was ~~false~~ a misunderstanding. The only agent information used in breaking wheels 1,2,3 was provided by the French (Bertrand from German traitor "Aschè"), and consisted of key sheets.

compromised machine. Since it was no longer possible to indicators,the chance of a depth crib became still more few depths were discovered,let alone read.

News From Poland

The preceding pages roughly indicate the lines of attack in the first six months of 1939. Within another month the whole position had been radically changed. At the end of July Knox went to Poland and met the cryptographers there; he returned with the startling news that the Poles had, with varying success, been reading Enigma for several years.

It is historically uncertain how the Poles obtained the wiring of the wheels and machine, and it was not a subject on which they were very communicative. Certainly they made extensive use of secret agents and it is most probable that they obtained photographs of keys and messages with clear-text. The essential fact that the machine diagonal was alphabetical they admitted to have discovered through one agent,though they claimed, no doubt with justice, that "nous avaurions pu trouver par mathematique". However much the Poles had depended on agents for their basic information there is no question that they were highly talented men, and that, with limited resources, they had performed brilliant work. In the course of the

part these months additional information was given about their methods of breaking and finally, at the beginning of October, we received a reconstruction of the Enigma itself. Owing to some uncertainty over the wiring of the two wheels with turnovers J/K and X/I was interchanged, a confusion which was later to cause us a certain amount of worry, fortunately short-lived.

1.116 Polish Methods of Key-breaking.

The methods of key-breaking adopted by the Poles are such as readily suggest themselves. There were essentially two methods, corresponding to the two different indicating systems. To consider first the original system, with settings doubly encyphered at a fixed Grundstellung. In the first place the message settings and the alphabets at the six positions following the Grundstellung were found in the way we have already described. The boxes of alphabets 1 and 4, 2 and 5, 3 and 6 were formed and their "shapes", i.e. the lengths of their separate cycles, noted. These boxes are of alphabets through the steckered machine, but it is clear that stecker have no effect on the shape of the boxes of the alphabets at two given positions, and that the actual boxes themselves can be obtained from those formed for the unsteckered machine by imposing on the latter the transformation represented by the stecker. The Poles therefore had catalogues of the box-shapes of unsteckered alphabets three apart for all positions and each of the six wheelorders(there were only three different wheels when this indicating system was in use). From these catalogues they could determine possible values for the wheelorder and basic setting of the Grundstellung(i.e.the setting relative to some standard ringstellung); namely, machine positions for which the boxes of alphabets 1 and 4, 2 and 5, 3 and 6 following had the required shapes. Such a solution having been found,the steckered alphabet boxes would be matched against the corresponding ones for the unsteckered machine; in this matching cycles of the same length would be "slid" against each other and the correct position would have to yield a reciprocal correspondence, the stecker transformation, between the letters of the boxes under comparison. This requirement was a severe one, so that from the possible solutions given by the catalogue the correct one could quickly be picked out. The solution thus found gave the wheelorder and stecker;to complete the key it was necessary to find the ringstellung. To do this it was sufficient to determine the basic setting(referred to the standard ringstellung) of any one message, the key ringstellung being the difference between the(known) tyre-reading and this basic setting. This was performed by rodding a short crib,such as the common beginning ANX. With the stecker known such a crib could be translated into a crib through the unsteckered machine. For each assumed absolute starting position of the right-hand wheel the constatation of this crib could be transformed,as previously described,into rod pairings through the two left-hand wheels and reflector(since the tyre-readings are known,so are the positions at which the middle wheel turns over, so that these can be avoided or taken account of). Of the 26 sets of rod pairings thus obtained further examination would first be made of those with confirmations(the same rod pairing arising from two or more constatations.) The absolute positions, if any, of the two left-hand wheels which gave rise to such a set of rod pairings could be obtained by reference to a catalogue of pairings through two wheels and reflector(it is not clear if the Poles had such a catalogue)or, with only 26^2 positions to try, simply by trial and error. Any such possible absolute setting thus determined for the three wheels could be tested by further decoding, and a correct one would immediately determine the key ringstellung.

When the new indicating system was introduced(with the message setting doubly-enciphered at an arbitrarily chosen setting, the outside indicator of the preamble)a method of attack was worked out which was based entirely on the weaknesses inherent in the system. It made use of a mechanical device known to us as the CYCLOMETER. This consisted essentially of two unwired Enigmas(whose wheels were turned by hand)wired together so that the output of each went straight to the input of the other. The circuit, which contained a lamp-board,was completed by pulling an appropriate switch on a board containing a switch for each letter of the alphabet. We have seen how the boxes of the alphabets at two machine positions break up into even cycles. Thus if the alphabet at one position contains the pairs AN, CY, DF, GH and that at the other contains the pairs AI, CD, FG, NY, the box will contain the 8-cycle(A X Y C D F G H), successive pairs of letters in this cycle being pairs of the two alphabets alternately. If the two enigmas of the cyclometer were set at the two positions concerned then the depression of the switch corresponding to any one of the letters of this cycle would light up the lamps attached to each of its letters,and only those lamps. In particular if the alphabets at the two positions had a common pair, say IM, then (IM) constituted a 2-cycle and only the lamps I and M would light up when either of the switches I or M were pulled. The chance of two alphabets having at least one common pair is about two-fifths:when it happened the two machine positions were said to be "female" with respect to each other.

Suppose now we have a message whose outside indicator and indicator groups are

A M K X C P X O R

At each of the positions A M L, A M O(referred to the unknown ringstellung) the letter X has the same encipherment,namely the first letter of the unknown message setting. These positions are "female three apart"; the distance of three was commonly tacitly understood and we should say "there is a female on X at A M L". In this the machine is steckered; if we are considering the alphabets through the unsteckered machine at A M L, A M O we can say that these alphabets have a common pair,namely the letter steckered to X and that steckered to the first letter of the message setting.

The procedure then was to pick out a number of these females, preferably on the same letter,from the indicator groups. The absolute settings were of course unknown,because the ringstellung was unknown,but the relative positions were determined by the outside indicators. Wheelorders were attacked in turn,the total number to be tried possibly having been reduced by the wheel-list previously described. A ringstellung was first assumed and cyclometers set up for each of the female pairs of positions. If these all proved to be genuinely female,this ringstellung gave a possible solution for further examination. Otherwise a new ringstellung was tried and so on through all 26^2 possibilities; the effect of a change of ringstellung could of course be obtained by the appropriate rotation of the Enigma wheels in all the cyclometers, the relative positions of any two Enigmas remaining unchanged. One person could operate each cyclometer, testing for female positions by the switchboard. A ringstellung hypothesis for which all the cyclometers simultaneously registered females was a possible solution. Among the letters shown up as female by a particular cyclometer there must occur in the correct position that steckered to the repeated letter of the associated indicator group; with several females on the same letter, therefore,the rejection of wrong positions was usually fairly rapid.

In any case a possible solution gives, in addition to the ringstellung, sets of possible stecker for the various female letters; and since from a hypothesis of the stecker of any particular letter we can, by virtue of the indicating system, deduce the stecker of a letter three apart from this in any indicator group, the rejection of wrong hypotheses for the female letters and the building up of the complete stecker in the right case was a simple if laborious process.

This method of solution, though essentially simple, required a high measure of concentration, and, in the absence of a powerful reduction in the number of wheelorders to be tried, it was intolerably expensive in man-hours. The Poles therefore were casting about for some more economical exploitation of the female letters of indicator groups; the solution they arrived at, the method of the Netzverfahren, was adopted by us: it will be described later.

1.12 WAR : THE FIRST SUCCESSES

1.120 The Outbreak of War

Within a month of the declaration of war we had thus received full particulars of the machine from the Poles, together with a reconstruction of the machine itself. At the same time they told us, however, that the Germans had changed everything at the outbreak of war. Although they advanced no evidence for this statement and gave no details, it was so intrinsically probable that we were prepared to believe it. It was obviously right to proceed with the assembly of apparatus for breaking, even though this might yield us only the decodes of pre-war traffic. While this was being done an intensive examination was made of current traffic for external evidence of the method of encipherment. At first, probably because of the lack of adequate wireless cover, it did seem that there had been a change of indicating system, but as the evidence provided by the goal-hunt accumulated it became fairly clear that this was not the case; and it also became reasonably certain, from the same evidence, that the Germans were still using wheels with turnovers at the old places. This did not of course mean that there might not have been a change in the wiring of wheels or reflector or both, but at any rate our confidence was somewhat restored.

Meanwhile a certain amount of practice was obtained in the breaking of traffic of the previous year which employed the old indicating system with fixed Grundstellung, and for which there were only six wheelorders to try, the possible permutations of the three original wheels. There was also at least one notable achievement in breaking on the rods from a small crib deduced by depth-reading. Rodding, as we have so far described it, is a method for discovering the wheels and their starting positions from a crib on the unsteckered machine. With more finesse and considerably more work, it can, however, in certain favourable cases be adopted when the machine is steckered. In addition to the assumptions of right-hand wheel, rod position and middle wheel turnover position it is necessary to make hypotheses for the stecker of one or more letters; the technique is thus, from all these hypotheses, to deduce rod pairings and the stecker of other letters. Full details will be found in the articles in the technical volume on Rodding and S.K.O. (Stecker Knock-Out), but a simple example will sufficiently illustrate the basic ideas involved. Suppose we have on the steckered machine the crib

. . . P C B P M A Q R . . .
N U L L

and that we are investigating simultaneously the stecker hypotheses P/A, B/N; suppose further that the right-hand wheel is known, that the middle wheel does not turn over in the stretch under examination, and that for the L constatation the right-hand wheel in at a definite position, say position 3, relative to the standard ringstellung. We have then to choose the rods which have A(the stecker of P) and N(the stecker of N) in the third position. Suppose there are the rods m and x. These rods - they were written out on strips of cardboard or wood - are laid in groups under the crib thus:-

P C B P L A Q R . . . ,
N U L L . . . . .

Rod m -Q Z A X N R E S L M . . . ,
Rod x -U L B V E S P C Y U . . . ,

Under the B constatation the rod letters are N. By hypothesis B is steckered to N; if therefore we are correct in all our assumptions it follows that L is steckered to E. Having now the stecker P/A, L/E we can lay the rods for the P constatation, namely the rods with A and E in the sixth place. Also under the fifth letter of Enigma text, L, the letters of rods m and x are P. Since L/E is a stecker pair it follows that the corresponding letter of clear-text is steckered to P, and is, therefore, A. This suggests that the crib can be extended to N U L L A (Q T).

This example illustrates the possibility of making further deductions about stecker and rod pairings and also how one can read or guess at clear-text beyond the crib. The process is clearly cumulative. If enough rod pairings are established for a given stretch it may then become possible to discover by reference to a catalogue or otherwise, for what left-hand and middle wheels and for what positions of these wheels these rod pairings are valid; a solution of this last problem immediately gives us all thirteen rod pairings, with consequent possibilities for further stecker and clear-text deductions.

The great number of different initial hypotheses to be tried makes a hand-break on the above lines normally impracticable without a very long crib. The Germans, however, introduced the device of stecker, like other devices in the years to come, in piecemeal fashion. It was not until 1940 that the practice of having ten stecker pairs to a key became general. In 1938 there were usually only four or five, with a probable increase to seven or eight in the latter half of 1939. With only a few steckered letters, therefore, there was a strong chance that any particular letter was unsteckered, or "self-steckered", as it was often called; thus the probability of the correctness of hypotheses could be judged by the number of self-stecker deductions to which they gave rise.

1.121 The Bombe and the Netz

Two instruments for solving were soon under consideration and development, the Bombe and the Netz. The former of these, a piece of high-speed electrical machinery, was far wider in its scope than the latter. It was designed to break a day's traffic either on the indicators or by means of a crib, while solution by the Netz depended entirely on the continuance of the indicating system then

in force. Bombe theory, however, was only in its infancy, and it was obvious in any case that a long time must elapse before theory, however sound, could be translated into an efficient machine. The Huts, on the other hand, presented few technical problems in the preparation of apparatus and approved a theoretically sound method of solution which should be ready for regular operation within a reasonably short time. Preparation of the Huts was therefore a most urgently important work and this was early put in hand. Nevertheless, since the Bombe, in its finally perfected form, was far and away the most important piece of apparatus used by Hut 6, it would be as well to describe simply at this early stage of its history, when it existed only as an idea, what exactly it was designed to do and how it was proposed to do it. Suppose we have a crib for the beginning of a message:-

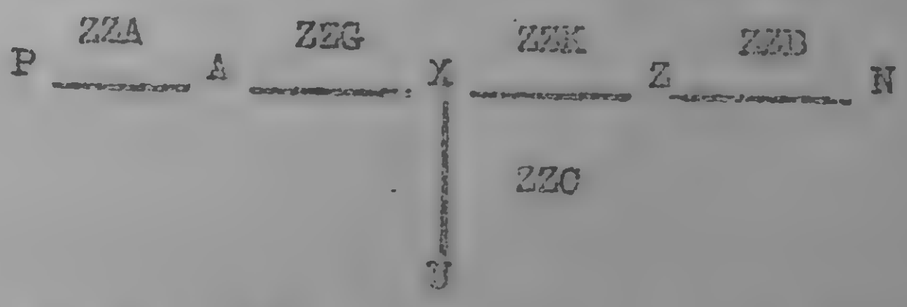
P Z U M L O A R E Y Z M L D C E E X V B R K U . . . . . .
A N X I F L X K D O X E I N S S I E B E N . . . . . .

There are normally sixty wheelorders to be tried; let us suppose we are testing a particular one. The absolute wheel position is unknown for any constatation, for we know neither the ringstellung nor the individual message setting, both of which are necessary to determine absolute position. We do, however, know the relative machine positions for any two constatations. This statement is not perfectly true because of the turnover uncertainty. Thus normally the two consecutive constatations $\frac{P}{A}\frac{Z}{N}$ occur at machine positions 1 apart; if, however, there is a turnover of the middle wheel between the two it is proper to say that the two machine positions are 27 apart, and similarly allowance must be made for the possibility of a simultaneous rotation of all three wheels. It is clear, however, that a sufficient number of hypotheses about the position or approximate position of the turnover will account for all possibilities; for the examination of any particular hypothesis, therefore, it is legitimate to assume that the statement above is correct. For simplicity we assume that there is no turnover of the middle wheel in the crib stretch of the example.

We first assume that the absolute wheel positions (referred to standard ringstellung) of the successive constatations are ZZA, ZZB, ZZC, etc:-

ZZ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z - - - - - -
P Z U K L O A R E Y Z M L D C E E X V B R K U - - - - - -
A N X L F L X K D O X E I N S S I E B E N - - - - - - - -

The different constatations can be formed into a linkage of which we show part, with the assumed wheel positions written on the links:-



If, say, R is enciphered by S at position ZZA of the unsteckered Enigma, then the stecker hypothesis P/R implies the stecker A/S. If now S and V are paired through the unsteckered Enigma at ZZG, we deduce from A/S the further stecker X/V and so on; an initial stecker assumption for any letter of the linkage implies the stecker of all the other letters of the linkage. Suppose now the links to be

replaced by Enigmas set at the appropriate positions,and that the output of the Enigma at ZZA is wired straight into the input of that at ZZZ, the output of this into both the Enigma at ZZK and that at ZZC,and so on. Then,given suitable recording devices,we can see,without attempting to go into technical details,that by putting in electric current at a given point of the first Enigma, or in other words,by making a definite stecker assumption for P, we can read off the stecker of all other letters of the linkage. Should we thus get a consistent stecker "story" we shall,if it is the right one, be able to check our results and obtain further stecker either from crib constatations not used in the linkage or by further tentative deciphering of the message: from the complete stecker to the complete key is a short step which need not detain us here. If the story is inconsistent we must make a different stecker assumption for P, and, when all 26 have been examined, proceed to a new set of wheel positions,the relative positions of any two Enigmas remaining unchanged. For each particular wheelorder and linkage there are thus 26×26^3 or 26^4 hypotheses to be tested.

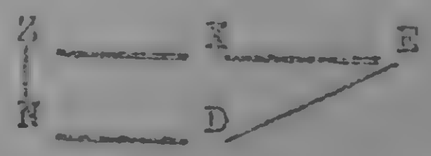
This, then, very roughly, is the Bombe, a set of Enigmas which could be plugged into each other according to a predetermined linkage. The Enigmas were to be electrically driven, moving on to a new set of positions automatically when all stecker hypotheses had been examined(also automatically)at a given set of positions.

So far we have considered a linkage obtained from a crib,but it is readily seen that the message indicators themselves provide material for such a linkage. Thus a message with outside indicator and indicator groups

	A M K	S U T L Q Y
gives the links		
S	AML ?	AMO L
U	AMK ?	AMP Q
T	AMN ?	AMQ Y

The letters here indicated by queries are the unknown letters of the message setting. There is no objection to joining such links as the above together to form a linkage for investigation by the bombe. Twice as many Enigmas are needed to form an equally powerful linkage (the power of a linkage being measured inversely by the number of solutions that it admits), but on the other hand we do not have to make different hypotheses about the turnover positions of the two right-hand wheels since, for any particular wheelorder,these are determined by the outside indicators:further the correct bombe story immediately determines the key ringstellung.

For the bombe as originally designed it was necessary that the linkage should consist of several closed circuits with a common letter. For the crib of our example such a closed circuit is the following:



At a given set of Enigma positions an initial stecker hypothesis for E, when taken round the circuit in a given direction will yield in turn stecker deductions for D, N, Z, X and finally E again. For the correct hypothesis the two values for the stecker for E must be the

some, a chance of 1 in 26. With four such closed circuits through E we expect on average one set of Enigma positions and one stecker for E which will satisfy the requirements for any particular wheelorder.

For a bombe on these lines it was hoped that it would be unnecessary to make 26 different stecker assumptions for E each time. A definite assumption, say E/F, would be made. If this happened to be correct, well and good: if not, it would lead, after one passage round the circuit to different stecker for E, which again would travel round the circuit and yield further stecker. In this way all letters other than F would also be deduced as possible stecker for E except possibly one particular letter, say R, which could not be reached from the initial (wrong) assumption; E/R would then be a potential solution.

The notion just described gets over the need for making 26 stecker assumptions at each stage. In other respects, however, it is extravagant in that it requires a particular kind of linkage which it might not always be possible to construct, and also in that the possible correctness of a story is based on the examination of the stecker of one particular letter. It takes no account of the fact that a stecker hypothesis for one letter implies stecker deductions for all other letters of the linkage; the requirement that all these deductions should be logically consistent with themselves and with the original hypothesis is a much more stringent one than that considered above. What then was really needed was a device which, without sacrificing the advantage of making all 26 stecker assumptions for a particular letter effectively in one, would make use of all the information that could be deduced from the linkage. It was the solution of this problem that characterised the great advance in bombe theory which was to be made in the spring of 1940.

Before leaving this subject for the time we may perhaps give the origin, possibly apocryphal, of the actual word "Bombe". The Poles are said to have had in mind a rather Heath Robinson device for dealing with the problem in which the signal of a potential solution would be the dropping of a heavy weight to the floor; this weight was the bomb, or, in the French which they used for communication with us, "bombe".

The bombe, however, was still very much in the air and the Netz held the centre of the field. We have described how the Poles, armed with cyclometers, attacked the weak points of the indicating system. It was clear, however, that the method was clumsy and extravagant in that every attack involved a fresh search for female positions three apart. What was wanted was some method of recording these positions for all wheelorders in a form which could be readily applied to the solution of a particular problem. After a good deal of consideration it was found that the Netz, now to be described, represented a reasonably simple and manageable solution of the problem.

The Netz were square sheets of paper (other materials were experimented with but not used in practice) in which the required information was recorded by punched holes. For each wheelorder there were 26 sheets, one corresponding to each position of the right-hand wheel. Every sheet was divided into four squares, each of which in turn was divided into 26 x 26 smaller squares identified by row and column letter. Suppose for the wheelorder considered, the position

Joan Murray (née Clarke)

Comment by JELM (23-2-78)

As I understand it, from memory + Prof's Book (written in 1940), this description does not apply to any stage of bombe design. The original plan for simultaneous scanning (i.e. testing all 26 stecker assumptions at once) did not rely on one passage round the circuit leading to a different ~~input~~ stecker for the input letter and thus to another passage round the closure(s). "Pye simultaneous scanning", being the engineers' planned implementation of the problem as put to them, used 26-phase power supply for the 26 assumptions.

The other, i.e. the logic for simultaneous scanning using the diagonal board, was only discovered (by Alan Turing) after Gordon Welchman's idea of the diagonal board for the purpose of getting "the complete set of consequences of a hypothesis .... to reject any position in which ~~the~~ a certain fixed-for-the-time Stecker hypothesis led to any direct contradiction" including on a ~~disconnected~~ secondary chain.

DXL(referred to standard ringstellung ZZZ)was female with the position DXO, 3 further on. This fact would be recorded by a hole punched in sheet L in the square with row D and column X.This hole would actually occur at four places in the sheet.the four big squares of the sheet being duplicates of each other. All the holes were punched by hand by a team of girls, the female positions * having previously been marked in on the sheets. These positions were determined by a machine known as the MOUSE in the form of strokes printed on master sheets. The accuracy of the top line of each sheet produced by the Mouse was tested by WATERMEEL, a device operated by the turning of a handle one person turning and another checking the female positions which were indicated by the flashing of an electric bulb. The tediousness of the latter work was enlivened by the discovery that the operation could be performed to waltz time.

The preparation of the Netz occupied a considerable time.The writer arrived at Bletchley Park in the middle of December 1939, just in time to assist at the ceremonial(and somewhat eccentric)punching of the two-millionth hole by the then Director(the podant will discover for himself that a complete set of Netz contains less than 2,000,000 holes; the discrepancy can be attributed either to pardonable exaggeration or to the fact that a second copy was being produced for the use of the French cryptographers,now strengthened by a contingent of Poles, who had made good their escape).

1.122 The Jeffreys Sheets

Before going on to describe the method of using the Netz we may briefly mention here the Jeffreys sheets +, which were also produced in the first few months of war. These recorded,also in the form of punched holes,the pairings through two wheels and the reflector. There was one sheet for each pairing containing 26 x 26 rectangles. Each rectangle had a row and column letter corresponding to the position of the two wheels,and the rectangle itself was divided into 5 x 4 squares corresponding to the 20 possible wheelorders. A hole punched in one of these squares thus indicated a wheelorder and wheel position for which the pairing written on the sheet was valid. The information to be transferred to the Jeffreys sheets was first recorded in catalogue form, one to each wheelorder. (The five wheels I to V were known by the colours Red, Purple, Green, Yellow and Brown respectively. The wheelorders 135, 234 etc., were called ROGOB, POGOY etc.; the catalogues of pairings through two wheels and reflector BOGOX, POROX, NOPOX and so on). The use for which the Jeffreys sheets were intended will readily be guessed. If an attack based on rodding on the right-hand wheel alone yielded a possible solution requiring, say, the rod pairings al, eg, hx,...., the sheets AL, EG, HX ... would be superimposed; any hole right through would indicate a possible combination and positions of the first two wheels for which all these pairings were valid. In practice the vulnerability of the indicators made the rodding attack unnecessary even if it should ever be possible,and for long the bulky cupboard-full of Jeffreys sheets languished unused. Later on in the war, when the Netz had become historic relics,the Jeffreys sheets came into their own for a few halcyon months,when an unintentional gift of stecker by the enemy made rodding once again a practicable technique.

* We use"female position" here and later to mean a position female with that 3 further on.

+ These were named after John Jeffreys,one of the pioneers of Enigma breaking.

1.123 Method of Using the Nets

The cyclometer attack, as we have seen, was a method of finding a wheelorder and ringstellung for which a certain number of positions(strictly,pairs of positions three apart)were female. The Nets provided a much simpler solution of this problem.

Suppose the indicators from a day's traffic on a given key yielded 8 or more female positions(8 was generally considered the necessary minimum: otherwise, unless the number of wheelorders could be drastically cut down, either by the goal-hunt or by the CILLIES later to be described,there would be too many possible solutions for convenient testing). For each assumed ringstellung of the right-hand wheel we took the 8 sheets(of the wheelorder set that we wished to try)for the corresponding absolute positions and superimposed them, staggered horizontally and vertically with respect to each other. The relative stagger between any two sheets was, horizontally, the distance between the left-hand wheels, and vertically, the distance between the middle wheels for the two females concerned. The sheets were set by means of a simple grid of squared paper fixed at one corner of the table. Any hole through the 8 sheets gave us 8 female positions for that wheelorder which had the required displacements relative to each other. This was a possible solution for further testing; it gave us the ringstellung at once, and the determination of the stecker and the correctness or otherwise of the position was soon performed by hand on cyclometers.

1.124 Early Failures

We have already described how a limitation of the possible wheelorders could be obtained from a comparison of the indicator groups of messages with adjacent outside indicators. All the outside indicators of a day's traffic on one key were recorded on a Foss sheet(a sheet divided into 26 x 26 rectangular compartments each identifiable by a row and column letter). Thus ABC would be recorded by the letter C and a message reference number entered in square AB. A routine examination was made of this Foss sheet for pairs of outside indicators capable of leading to goals, that is such that the machine positions for the encipherment of the six-letter inside indicator would overlap by 4, 5, or 6 given a suitable wheelorder.

Several days' traffic after the beginning of the war had good wheelorder reductions and a sufficiency of females,so these were attacked first. It so happened, unfortunately, that these all involved wheels 4 or 5 and, owing to the mistake about the turnover positions of these wheels,both the wheelorder deductions and the setting of some of the sheets were at fault. Some half dozen days were tried altogether,through all 60 wheelorders when the goal evidence did not positively reject any wheelorder. One after the other they went down and a general gloom descended. Within a few weeks it was lifted again when an emissary took a duplicate set of Nets to Paris and there discovered the confusion between the two wheels. These few weeks were not, however, wasted, for it was in this time that the existence and importance of CILLIES were first recognised, a discovery of far-reaching consequence.

1.125 Cillies and Attempts at Depth-reading

These repeated failures made us fairly certain that the Germans had after all introduced some innovations at the beginning of the war, the most popular guess being that they had brought in a new reflector.

In order to break this we needed a long crib,and the only way to get a crib was to read a depth. It ran as a means to this unlikely end that we first expected cillies to be most useful.

From the decoding of pre-war traffic it was noticed that the German operator often took as his outside indicator the final position of the three wheels at the end of the preceding message; by so doing he saved himself the trouble of altering the wheels for the encipherment of the message setting. Since the message setting was often obviously selected, either as a "keyboard" like FVK, DFG, CGU, etc., or a "pronounceable" like HAN, WAL, MAR, CIL, etc., it was possible by "subtracting" from the outside indicator of a message the number of letters in that preceding(excluding the 11 letters of the discriminant and indicator groups) to find what the setting of the preceding message was,on the assumption that "cillying" had taken place. (The pronounceables were often the first three letters of a proper name, e.g. MARtha, WALter, CILli, and it was this last which gave the name to the process,since CIL was the setting of one of the first messages in which the practice was observed). The result of the subtraction depended of course on which wheels were assumed in the middle and on the right, and therefore a correctly guessed cilli generally implied a reduction in the number of wheelorders.

Looking for cillies became a popular pastime and, though at first we over-estimated the amount of cillying and believed cillies that we should later have been very sceptical about, we did nevertheless get impressive-looking wheelorder reductions on some days. We did actually, in our enthusiasm, suspect that new wheels were in operation because on some days we could find no cillies on the old turnover assumptions. On one such day one of us deduced the existence of a new wheel with two turnover notches; if such a wheel were assumed a noble array of cillies was obtained. It must be said that this hypothetical wheel did not command general belief. The actual subtraction was first done by the sliding of measuring strips (the number of units of length being the number of letters of the message) against a long strip consisting of the alphabet written out several times; these "snakes" were clumsy,and later we used a simple subtracter involving a transparent numbered grid 26 units wide and about 10 deep(to allow for a message length of 260)which could be slid over a 26 x 26 card in which each square had its appropriate row and column letter entered. Finally, when it became almost second nature to work quickly in the scale of 26,all such aids to subtraction were gradually dropped.

The attempt at depth-reading in order to find a crib on which to break the hypothetical new reflector was short-lived,but it was interesting practice. We chose a day with several good cillies and had all messages on the key punched out on "Banbury sheets" so called because they were prepared by a printer at Banbury. These were strips of paper on which were printed some 300 columns of letters, each column consisting of the alphabet written vertically. If, say, the 197th letter of the message were F, then a hole would be punched in row F, column 197. The process of counting the repeats between two messages at a given staggered distance could be easily performed by superimposing the sheets and counting the holes through both. The sheets for each message were labelled with reference number and cilli value, if any. All messages with good cilli values like WER were counted level with the rest; any which gave a count considerably better than random could be tested further by counting them,at the appropriate stagger, with the several WER's which were the basis of the story. Messages with cilli values near WER were counted against this both level and at a stagger of, say, 1 to 50 either side to see

whether anything remarkable showed up. However, in the end, we did not succeed in getting anything better than a rather dubious depth of about seven,which was quite impossible to read.

1.126 The First Breaks of War-time Keys

The attempt at depth-reading was abruptly terminated at the end of the year when our emissary returned from Paris to tell us of the muddle between wheels 4 and 5 and with the great news that a key had been broken(October 28 Green) on the Netz sheets he had taken with him. Immediately we got to work on a key(October 25 Green) for which, by cillies and goal-scoring, the wheelorders had been convincingly reduced to three only; this, the first war-time Enigma key to come out in this country, was broken at the beginning of January 1940.

We eagerly awaited the opportunity of finding the answer to the next great question: Had the Germans made a change in the machine at the New Year? While we awaited a suitable day,that is one with enough females for our purpose,several other 1939 keys were broken and we began to get evidence of the extent and nature of cillying. At last the favourable day arrived, and it had, besides the requisite number of females, several good cillies to cut down the wheelorder. The sheets were laid, the stories tested, and Red of January 6,1940 was out. Other keys soon followed and Hut 6(at the beginning of January we had moved from Elmer's School into a new wooden building) was beginning to get into its stride.

CHAPTER 1·2

PERIOD II: JANUARY TO JULY 1940 : SITZKRIEG, NORWAY, FRANCE : START OF CONTINUOUS OPERATIONAL BREAKING

1·20 FIRST ATTACKS ON KEYS

1·201 Red, Blue and Green

As we have seen it was not until January 1940 that there was any success to current breaking in Hut 6. It was not until then, in the later third of the year, that we reached the stage of continuous current breaking on any key. The position in January 1940 was as follows. Our resources in sets were not sufficient to enable us to intercept large quantities of traffic and indeed it is certain that in comparison with later periods no great volume of traffic was being passed just now. Nevertheless three different keys (or colours)* were thus early recognised - Red, Blue and Green. These are the three 'primaries' among the more or less two hundred keys that Hut 6 was to recognise, unravel and break.

Of these keys Red, the general C.A.P. key, was recognised a few months later as the most urgent and important of all Enigma keys and retained this place for fully four years, during which it was broken daily with very few exceptions. Even in the last year of the war, though Red was dethroned from its intelligence primacy, it was still at the cryptographic centre of Enigma-breaking. There can be no question that Red was in general the most important and famous key of the war.

Blue was the closest analogy to Red among G.A.P. keys by virtue of its universal nature, but from any other standpoint far inferior. With rare exceptions its content was always practice messages - it was the Luftwaffenmaschinenübungsschlüssel. Compared with Red it was broken seldom largely because its intelligence value was almost nil: and in fact its dignity as one of the three "primaries" was very honorary in nature.

Green (known also as Yellowcake and later as Greenshank) presents a very different picture. In its own way it almost paralleled the renown of Red and it had the honour of confronting Hut 6 with some of its most difficult cryptographic problems. No colour that was so much worked on was broken more seldom and none had a higher standard of cipher security. Throughout the war Green was the key of the Wehrmacht or Army Commands into which the Greater Reich was divided. It would be false to claim that its position was the same as that of Red: there never was any general Army key as Red was the general Air key, but there are respects in which it was the closest Army equivalent to Red. There never was any other Army key which lasted for so long a period as Green and during all its life it was valid over an immense area.

1·202 Success and Early Organisation

The Vetter method proved in practice very effective and when breaks had once started they came rapidly. From January to March 1940 we broke some 50 keys of Red, Blue and Green, and this is not counting an appreciable number of 1939 keys that were also broken in this period. Every 1940 day broken had ten wheel patterns; the 1939 days all seven or eight. While we did not break a day between October 28, 1939 and January 6, 1940 it is not possible to suppose, in view of what was later discovered about the systematic habits of the Germans, that the change to five wheels took place on January 1, 1940.

* Keys were originally distinguished by arbitrary names - I cannot recall the use of "colour" as a synonym for key.

The organisation of Hut 6 was at this time of the simplest. There was at present no necessity for a night shift nor sufficient staff to man it: so a two-shift system was in general operation. The sections of the Hut were as follows:-

N.R. (Note Room) engaged in "shoving the sheets";

M.R. (Machine Room) arranging the data in suitable form for the N.R., checking stories and completing the key;

R.R. (Registration Room);

D.R. (Decoding Room).

Looking for wheelorder tips by cillies was still regarded as an esoteric mystery. It was for a time presided over at "the Cottage" by Dilly Knox, assisted by occasional visitors from Hut 6. Knox had been the pioneer worker on Enigma in this country and his energy and enthusiasm had been an inspiration to all in the early months. When the Enigma had disclosed its secrets and Hut 6, under Welchman, was firmly on its feet, Knox and his Cottage party turned their attention to new problems.

1·21 OPERATIONAL BREAKING

1·210 Rise of Yellow

The first indication of the new era of operational breaking came with the Norwegian campaign. The invasion of Norway by the Germans resulted in the immediate rise of a new key passing considerable quantities of traffic. This phenomenon of the rise of a new key coinciding with the opening of a new campaign was often to be repeated and arose naturally from the German system of key distribution; when a new land campaign was planned the armies involved were allotted one or more keys (according to the size of the operation) and these keys came up in strength as soon as the campaign started. It also followed that on the successful conclusion of a campaign or on the establishment of land-lines in sufficient quantity the key might dwindle or even vanish as quickly as it had arisen.

These points are illustrated in the brief history of Yellow (as the Norway key was called) which lasted in quantity from April 10 to May 14 and was broken from April 15 to May 14 inclusive. Yellow continued to use the single indicator system even after other keys had changed to the new system soon to be described and the amount of traffic was large enough to make continuous and regular breaking on the sheets possible.

Yellow decodes in content referred to the G.A.F.: yet the key was technically an Army key i.e. one issued by the Army cipher authorities. This became clear later from several points, as, for instance, its key rules; at the time, however, the distinction between Air and Army keys could not be fully realised, and it was not till 1942 that it was quite clear they formed fundamentally different sets. It is odd in view of the fact that during the war Army keys were in general harder to break than Air keys that the first key to be broken continuously for a month was an Army key. But, of course, this was only possible because of its use of an indicating system already obsolescent.

1·211 The New Indicating System: First Great Triumph of Hut 6

On April 29th and 30th a new indicating system appeared on some of our traffic. This was called the double indicator system and was characterised by two (not one) three-letter groups in the preamble. In the message itself the discriminant group remained as before. Thus to all appearance the message proper began in the 6th place as in fact proved to be the case. It might be mentioned here that at a later date the Germans put the discriminant (if used at all) as a third trigram in the preamble and started the message in the 1st place.

The change did not come as a surprise: we had had in decodes clear warning that some change was envisaged. And here it should be noted that in cryptography it is impossible to overestimate the value of regular daily breaking, particularly in giving timely warning of any new complications the enemy is planning: and in fact throughout the whole history of Hut 6 there were extraordinarily few examples of any innovations in German technique of which we did not have adequate forewarning. It will be realised that in examining traffic we had always to be on the look-out for messages that gave information of this nature and as a safeguard it was arranged at an early date that Hut 3 should send back to Hut 6 for investigation any relevant "key messages", as they were called.

As soon as the first hints of a new system had been observed, speculation on its nature became widespread through Hut 6: and in fact the correct answer was soon guessed. It was thought that the first three-letter group was still the outside indicator and the second three-letter group must be the encode of the message setting starting from the position of the outside indicator. Fortunately it was easily possible to prove that this theory was correct because with crass stupidity the Germans on April 29th and 30th employed both systems simultaneously on Blue: so we broke on the old system and checked up on the new. In May all colours adopted the new system except Yellow which continued to use the old system till its demise, and was still broken by the Netz method.

At one blow a catastrophe had fallen. In the course of its history Hut 6 had to face many a crisis but from some points of view this was the most serious of all. In later crises we had at least a tremendous background of knowledge and experience of the whole German cipher system, a staff sufficiently large to undertake if necessary the most laborious hand operations, and a large reserve of complicated cryptographic machinery. But in May 1940 our whole system of breaking had been rendered useless at a moment when we had none of the above advantages. It is true that the bombe which still provided a solution to our problem (given a crib) was in production; but the first machine was not expected for several months yet - it arrived in August - and how were we to fill in the interval ? Besides if we did not make any breaks till then how could we expect to write out cribs when the bombe came ?

It was a godsend for the whole future development of Hut 6 that it so happened that in May and the following months German cipher security was so hopelessly bad that the enemy failed to reap the advantages they should have attained by the great improvement in their indicator system which they had carried out on the eve of their great Western offensive. Not for the last time the carelessness of German cipher clerks wrecked the well-laid plans of their cryptographers. Yet the severity of the crisis can be measured

by the fact that (apart from Yellow, which was on the old system) no key was broken in Hut 6 for a period of about three weeks - the longest gap in breaking from January 1940 to the end of the war. Still, had the German cipher security been anything like adequate we would have been fortunate indeed to get the first break on the new system within three months.

1·212 Overwhelming Importance of Red

On May 10th the German attack in the West altered the whole interception situation. After a two day's wireless silence traffic suddenly rose to hitherto unheard of dimensions and quick decisions had to be taken in view of our limited resources in sets. It was obvious from mere volume that one key - Red, the general G.A.F. key, - was of paramount importance, and the decision was made to concentrate on this key and drop everything else. There can be no doubt that in view of our cryptographic resources and the possibilities of breaking this decision was absolutely correct. It is almost certain in view of our later experiences that there was in existence at this time a large quantity of Army traffic of high intelligence value and readily breakable on the mechanical resources we began to get in a few months: but very little of it could have been broken in summer 1940 as these resources were not yet available and we were right to concentrate on what we could break. In what follows we shall sketch as briefly as possible the general theory of the hand breaks on which we kept going: a later section will outline the daily routine adopted but for the details of technique the reader must consult the technical volume.

1·213 Hand Breaks

It is, in general, impossible to break any Enigma key with an adequate indicating system unless one has a crib - using that word in its widest sense as the clear language equivalent of a section of cipher text. The hand breaks of 1940 depended on the use of a specialised type of crib - the cilli - combined with a severe limitation of the number of machine positions to be tried. A machine position means a wheelorder/ringstellung combination: there are 60×26^3 i.e. approximately one million such positions.

CILLIES have already been referred to, so it is only necessary to summarise the essential points which are:-

(1) A cilli occurs when a cipher clerk, after encoding a message, proceeds without moving his wheels to encode the next message i.e. when the ending position of one message is the outside indicator of the next message. The setting of the message is the cilli.

(2) If a cipher clerk has cillied, it is possible by subtracting the length of the message from the next outside indicator to arrive at the cilli - or, more exactly, to arrive at several alternative possibilities (according to the wheelorder assumed) for the message setting.

(3) As message settings were selected by the free choice of the German operators, they were often non-random and fell into a number of popular categories - e.g. keyboards, pronounceables, nearnesses and a few other groups. In 1940 such non-random settings were particularly common - in mobile warfare cipher security is the first casualty.

(4) So after subtraction we may be able to select the true message setting from the alternative possibilities (normally four) by recognising it as one of a favourite group. This gives us a three-letter crib and normally a wheelorder reduction. Of course, this recognition of the setting is the point of cillying i.e. subtracting messages in a search for cillies; and as normally used cilli means a recognisable cilli, one spotted by subtraction as at least possibly correct.

(5) Finally, a number of cillies on the same key make up a cilli story. They can be used together as the relative machine positions are known and their self-consistency in wheelorder reduction and possibly in type provides an internal check on their correctness.

But before a hand break can be considered there must also be a ringstellung reduction. Here we come to the RINGSTELLUNG TIP, also named Herivelismus after its discoverer, J.W.J. Herivel. It appears that it is in accordance with human nature when setting up a key in a machine (1) to put the right wheelorder in the machine and then (2) to set the clips in the right position. These steps can be taken in the reverse order, but the order given above was in point of fact normally adopted by Hut 6 and obviously also by German cipher clerks.

Now it is quickly seen by experiment that if the ringstellung is set up after the wheels are in the machine then the reading showing in the window is near the ringstellung. If in addition the cipher clerk encodes his first message without moving his wheels then the outside indicator of his first message is somewhere near the ringstellung - in practice it tended to be either "dead" i.e. exactly right or completely "in step" i.e. with each letter of the alphabet the same distance on or back. Thus it was sometimes possible to deduce the ringstellung exactly or within narrow limits from an examination of the first messages of various operators. Once, for instance, on a Kestrel day the exact ringstellung was sent no fewer than five times and on March 24, 1943 Quince the first six messages on the blist had as outside indicators XMF, XMF, XMF, WMD, AFH, XNF, - the ringstellung being naturally XMF. It is clear that this is a kind of laziness strongly akin to cillying - both depend on the German operator not moving his wheels when on grounds of cipher security he should. It is thus not surprising (though it was very fortunate, especially in 1940) that cillies and ringstellung tips tended to arise on the same keys and often from the same men.

Now it is essential in attempting a hand break to have the number of positions considered worth trying severely limited, probably by cillies and ringstellung tips combined. How big a range can be covered depends to some extent on the material available: but even with ample material - i.e. a good cilli story - one would hardly undertake more than 180 positions at the outside and one might well think twice before tackling more than 60. During this period most hand breaks were on a much smaller scale: the normal minimum was three positions i.e. three wheelorders and a dead ringstellung.

Assume for the sake of argument that we are making a hard attempt and that we have been fortunate enough to try in the first instance the correct wheelorder and ringstellung i.e. the correct position. It should be clear that our problem is solved and that we have broken the day if we can find the stecker. So what we want is a method of working out the correct stecker when we know the

correct position and have a series of cillies, i.e. steckered constatations at known positions of the machine.

In practice it is very easy to do this by setting up a German machine to any of the positions in question and then using the principle of STECKER IMPLICATION - i.e. that if it is known that at a given position of the machine W decodes as E, then any assumed stecker of W gives rise to one, and only one, stecker of E. If, for instance, AG is a pairing through the unsteckered machine, then W/A implies E/G and W/G implies E/A. This is perhaps <u>the</u> fundamental principle of all Enigma breaking.

Thus by assuming any stecker for one letter we get the stecker of another letter and so proceed to a third and so on until we either get a contradiction (proving our first stecker assumption was wrong) or begin to get confirmations when we suspect the day is out. The correct story is always recognised by confirmations and self-stecker and it was in these early days a great thrill when this happened. In due course the miracle became almost a routine: and yet the magic of a hand break of Enigma never wholly faded into the light of common day.

It is obvious that for hand breaks any further limitation of wheelorder, ringstellung and stecker (beyond what can be deduced from cillies and ringstellung tips) is invaluable. Hence arises the practical importance of the rules of keys that were now discovered. But this subject deserves a section to itself.

1·22 THE RULES OF KEYS

1·220 General Considerations

The subject of Rules of Keys is a large theme that runs throughout the whole history of Hut 6 from the summer of 1940 to the end. Sections on it will therefore be found in each of the subsequent periods and a reader who wishes to trace the historical development of the whole subject is advised to peruse these in succession. The present section is a general introduction including the initial discoveries of summer 1940.

Even as early as the spring of 1940 before continuous breaking had started several people in Hut 6 had already started looking for rules of keys - i.e. had begun to examine meticulously the various keys broken and try to find any sort of pattern in their construction. Of course, the main difficulty in this kind of research is that one does not know precisely what one is looking for; to know this one would have to have guessed the rule already. All one can do is to arrange the available material in any way one can think of that might be helpful and then examine the results.

The psychological nature of the investigation is pronounced. What one is looking for is an insight into the mind of the German keymaker: to discover the rules or principles by which he works. There are numerous pitfalls in this search of which three may be mentioned.

Firstly, the sceptic might doubt whether there are any rules at all. There is no absolute necessity why keys should be made up on any system: why should they not be absolutely random ? The answer to this difficulty lies not in logic but in psychology. It seems to be an inherent trait of human nature - and not least perhaps of the German people -- to seek to introduce system even where there is no need or desirability for system to exist. This explains both why rules of keys exist and why (despite all sceptical arguments) people persist in looking for them. In short, the ideal of randomness is as difficult for the layman to achieve as it is for the mathematician to define.

The second difficulty is that it is not necessarily easy even when an apparent rule is discovered to look at it from the same angle as the enemy and to express it in his way, and unless this can be done, we may not appreciate the full significance of our discoveries. A good example of this is the Nigelian wheelorder rule discussed later. It was discovered that most G.A.F. keys took their wheelorders from what appeared an arbitrary list of 30: the question at once arose whether this was the whole story or whether there was behind this rule an elaborate system of picking the order of the wheelorders, whether in fact this apparent rule was merely a consequence - possibly an unassigned consequence - of some system which we never understood.

The third difficulty is more obvious: the difficulty of distinguishing a rule in the strict sense - i.e. a regulation observed by the keymaker - and a mere tendency. This can only be done on the basis of much evidence of broken keys considered in accordance with the laws of probability. It must be remembered that a strong tendency even if of short duration may be almost as useful as a rule.

It has been mentioned above that the first investigation into the actual keys we had broken began in spring 1940. Then, however, no progress was made and in fact none could be expected as there was not sufficient material on which to work. In general, nothing much can be done in this sort of investigation until there is about a month's keys - as complete as possible - ready for analysis. It also happened that the original tentative investigations considered the whole key as a unity, and we were soon to see that this was the wrong method.

1.221 The Rules of Red

From May 20th onwards Red was broken daily for months, and indeed years, on end: and it was not long before rules were discovered for each of the three constituent elements of the key - wheelorder, ringstellung and stecker. All the rules to be now described were discovered in June 1940 and confirmed on the evidence of May and the following months.

Wheelorder Red was found to obey both the non-clashing rule and the non-repeating rule. The first rule was that on any two consecutive days in the same month the same wheel could not be used in the same place. By this alone if one day was out the wheelorder for the next day was automatically reduced to 32 instead of the usual 60. The non-repeating rule, which was never quite so absolute, simply laid down that within a month the same wheelorder was not used twice.

Ringstellung If for the first 26 days of any month the ringstellung were written down in three columns, each column contained all the letters of the alphabet once and once only. Days past the 26th chose their ringstellung arbitrarily.

Stecker Consecutive stecker, i.e. A/B, C/D etc; were never used. Note that A/Z was allowable showing that the keymaker looked at the alphabet from a linear and not a cyclical viewpoint. Also the keymaker strove to avoid repeated stecker pairings in the same month. It was not possible to avoid such pairings altogether, for there were only 300 legal stecker pairings and it was proved by later events that all keys must have been made up as if for 31-day months: and the evidence supported the theory that repeats were allowed rather more freely with the first five days of the month.

1.222 Results of the Discoveries

These discoveries had two consequences: they were of immediate practical assistance in breaking Red, especially on the hand methods then in vogue and they definitely fixed the future lines of research into rules of keys.

On the first point the influence of the wheelorder and ringstellung rules in reducing the number of positions to be tried is obvious and about the 26th one had an excellent chance of firing the ringstellung dead: while the stecker rules greatly facilitated the picking out of the correct story by inspection from several plausible alternatives. Stories could be rejected out of hand on a consecutive stecker and it was a bad mark against them if they threw up stecker clashes. In fact the immediate effect of these discoveries was to lead to the quick breaking of several obstinate missing keys.

On the second point the concept of a key block became clear. It was obvious from the rules that the keys of a calendar month formed a unity to the Germans: we were to discover that each month's keys were issued as a whole on a keysheet and given a key number. Thus the future theory split into two sections - discovery of rules within a key block and comparison of different key blocks. This last section led in 1942 to the discovery of key repeats.

1·223 Rules of Other Keys

One further point should be stressed. The rules already discovered were valid so far as we knew for Red alone: they had later to be tested for each new key broken. By July 1940 we had, apart from Red, broken some Blue, some Green, a lot of Yellow and a single day of a key called Purple. How far did these keys obey the new Red rules ?

Often there was simply insufficient evidence. It looked, however, as if Blue obeyed the rule against consecutive stecker, while clearly Green and Yellow did not. Yellow also did not observe the non-clashing wheelorder rule nor the Red ringstellung rule. It had, however, been previously discovered that Yellow was using another ringstellung rule by which all the letters of the alphabet were used in blocks of approximately nine days as under:-

May	1	ALO
"	2	ENF
"	3	IBJ
"	4	GKD
"	5	CHM
"	6	NXA
"	7	HPU
"	8	OBZ
"	9	VLX
"	10	EWQ
"	11	IYC
"	12	LDR
"	13	SFJ
"	14	A)(KT

After the discovery of the Red ringstellung rule this was put aside as an oddity: but it was to reappear later and be known as the Army ringstellung rule.

1·224 Red Keys, June 1940

To illustrate the above points the Red keys for June 1940 are now appended.

DATE	WHEELORDER	and RINGSTELLUNG
1	514	GMP
2	321	RYK
3	215	VDG
4	531	NTZ
5	124	ZHB
6	312	EXO
7	423	TPJ
8	154	KBF
9	352	CRX
10	541	SIT
11	123	JUH
12	214	WAY

DATE	WHEELORDER and RINGSTELLUNG	
13	345	FWN
14	512	QLA
15	135	BGG
16	451	NOW
17	143	MSL
18	235	WCL
19	543	DJQ
20	341	OZC
21	152	INU
22	245	XEI
23	534	AVR
24	315	UKD
25	432	PFM
26	154	LOV
27	543	HDS
28	132	SXK
29	354	XGN
30	521	HPC

DATE	STECKER A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
1	F - M - S A P V - W Z Y C T - G - - E N X H J U L K
2	D - M A - J V T P F - X C - Z I U - W H Q G S L - O
3	K W T U L - - - S - A E Q P - N M Y I C D X B V R -
4	L K F - - C Y - - U B A R S X V - H N W J P T O G -
5	D I - A - V W M B - Q S H X - U K T L R P F G N - -
6	- Q X P S T - W Z Y N - K - - D B V E F - R H C J I
7	- S - G - W D - - Z R P O U M L X K B V N T F Q - J
8	F X - Y - A I Q G V T - - - S R H P O K W J U B D -
9	D K R A J Q N X L E B I Y G Z - F C - - - - - H M O
10	- - Z S V H - F - T Y U W R Q - O N D J L E M - K C
11	V H - W Q - S B Y - P - - Z - X E U G X R A D T I N
12	X - M - N R L Z V Q O G C E K Y J F - - - I - A P H
13	Q G J H X - B D K C I N V L U - A - - Z O M - E - T
14	W - Q N Y M T K R P H - F D - J C I - G Z - A - E U
15	T M V F Z D X J - H - - B Q R - N O - A - C Y G W E
16	H T - R W O - A U - X - P V F N Z D - B I N E K - Q
17	N I P M - J - U B F - N D A W C T L Y Q H - O - S -
18	O D F B I C K Y E N G Z T J A X - - - M - - - P H L
19	H R O J U X - A N D - - Y W C S - B P - E Y N F V -
20	C N A Q T P U L O - - H X B I F D Z - E C - - M - R
21	P - W O H Y R E X S - Q Z - D A L G J - - - C I F M
22	- V H Z G U E C Q R - O S - L - I J M Y F B - - T D
23	J L U R P K Z S N A F B - I Y E - D H - C - - - O G
24	U P E V C Z - N W L S J R H - B - M K - A D I - - P
25	M Z I L R S O - C - - D A - G T V E F P Y Q - - U B
26	E O Y I A - J - D G U - - T B W S - Q N K - P Z C X
27	Y J L T O N M R P B - C G F E I - H - D - - Z - A W
28	S U N X K - Q - Z M E T J C Y - G - A L B - - D O I
29	I Y G - M L C P A O N F E K J H - W Z - - - R - B S
30	Z F S K L B - O T - D E U - H - Y X C I M - - R Q A

In the above dashes represent self-steckered letters and repeated pairs (counting from the end) are underlined. Note that there are only 16 repeats and that 14 occur on the first five days of the month. Stecker pairings for a month were charted on a Foos sheet, a convenient method for throwing up repeats and showing what pairings were still unused.

1·23 DAILY PROCEDURE IN MACHINE ROOM

It may be helpful in filling out the picture of Hut 6 in summer 1940 if a brief account is given of the daily routine in the Machine Room which at this date was certainly the nerve centre of the Hut,

The M.R. worked three shifts:- 0000-0800, 0800-1600, 1600-2400[H] and there was sufficient personnel to provide three or four members for each shift. The main object each day was to break the current Red and this was frequently accomplished during the day shift and occasionally even before 0800 - the day when Red was broken on a hand attempt at 0500 was long remembered as a record at the time.

The traffic was examined in the first instance on the registers which were a continuous list of the messages by each station, giving the essential details of the preamble including the first two groups of the message. The Red discriminants were quickly identified and it was the custom for the registrar - the member of the shift whose primary responsibility it was to examine the register - to underline Red discriminants in a red pencil. This enabled one to see at a glance what messages were on the Red key and the practice was later extended to underlining other keys in appropriate or conventional colours.

The registrar also subtracted all messages, paying particular attention to known cilli frequencies, and noted any possible cillies he discovered. The listing of first messages and search for ringstellung tips was another important part of his work. A third was the AN-sheet, i.e. the fossing of the first two letters of all messages and the counting of any with an initial bigram.

The idea of this was to pick up depths, i.e. two or more messages encoded at the same message setting which would of course show this by a plain language count instead of a random count[θ]. The justification for the initial bigram test was the fact that in general the commonest single beginner to German messages was the word AN.

At a later date the AN-sheet was given up as being insufficiently productive of results: but in 1940 it paid good dividends. It is possible (as is shown in the technical book) to use a fit or banbury as it was called in a hand attempt and also if one of the message cillies we know the setting of the other one. In a period where cillying was plentiful and keyboard settings were frequently used, it was quite likely that fits would arise with keyboard cillies and in fact on one day no fewer than ten NMIs were discovered.

If as a result of the above investigations enough material was discovered for a hand attempt, this was organised forthwith, and if desirable the work was split up among the whole shift. (The methods employed are discussed in detail in the technical book). It should be understood that at this period the organisation was extremely informal, and there was none of the fairly rigid differentiation of function between the various members of a shift that later proved necessary: in general everything was a matter of ad hoc arrangement. Unbroken back days were considered by the same people who were attempting to break the current day.

H This three-shift system continued to the end, but for practical reasons the night shift later ended at 0900.

θ Figures were worked out later for the chances of various counts being genuine. Roughly speaking a depth should have a count of at <u>least</u> 1/18 instead of the average 1/26.

As can be guessed, with only one major key to break (and in fact only one key that was being taken in quantity) it happened that if Red came out early, the evening shift was unemployed so far as operational work was concerned. On these occasions the members of the shift occupied themselves in a more or less systematic way with any general problem that attracted them - in particular the discovery of the original rules of keys and the first investigations into what was to become known as "the dottery" were made in these quiet hours. It is never very easy in an expanding organisation like Hut 6 to get a perfect correlation between the work to be done and the staff available at any moment: one constantly has either too large or more often too small a staff for immediate needs. But the experience of 1940 suggests that, while in general once the organisation has got going on a large scale and the main lines of advance seem clear, it is preferable to have too small rather than too large a staff, there is a good deal to be said in the early experimental stages when the main technical problems are still to be solved for having a small excess of staff over strict operational requirements. At this stage if the right staff is available leisure time spent in free experiments is unlikely to be altogether wasted.

1·24 LIAISON WITH FRANCE

The subject of this section is rather by itself and not closely connected with any of the preceding sections; but it obviously deserves brief notice. The liaison to be described was not confined to the period we are now discussing but extends from the beginning of the war until the fall of France.

During all this time there was a constant interchange of cryptographic information between Hut 6 and the corresponding French organisation, and our allies were fully informed of the technical processes we were using and of our future plans - i.e. the bombe.

In particular, all keys broken by either side were interchanged and in fact one of the important days that established the new indicating system was broken by the French. The keys broken in France were, however, much fewer in number than those broken here; this was probably due to the fact that their mechanical resources were even more rudimentary than ours were.

When the fall of France was clearly imminent, this regular intercourse was naturally broken off and henceforward until liaison with America became an important factor in 1943, Hut 6 fought its war alone. It is obvious that had the war taken the course anticipated by the Allies in 1939, France would have played a significant part.

It can easily be realised that the fall of France caused much anxiety in Hut 6 not only for general reasons but for fear lest the Germans should find out that we had been breaking their traffic and the methods we were using. Such knowledge on their part would have been disastrous for our future success; for (apart from more far-reaching changes of the machine they might have brought into force) they would certainly have done something to eliminate cillies if they had realised their practical importance.

It is due to our allies to state that it is now clear from the lack of German security devices at this time that they secured no information of cryptographic value from the French: and so, fortunately for Hut 6, this dangerous moment (when the Germans had their best chance of securing an insight into our breaking methods) passed over without any appreciable damage being done.

CHAPTER 1.3

PERIOD III : AUGUST 1940 - MAY 1941 : BRITAIN ALONE : RISE OF BOMBES AND THE CRIB ROOM

1°30 GENERAL HISTORICAL SUMMARY

This vital period, corresponding to one of the major crises of the war, is the time when the foundations of Hut 6's success were at last firmly laid. It is the immediate prelude to the great central period of consolidation from June 1941 to December 1943 when an adequate solution was found for all technical problems that had presented themselves to that time.

But from this time on the complexity of the German key system and the complexity of Hut 6 organisation for breaking increase together: and it consequently becomes more and more difficult to treat the subsequent periods in strict historical sequence. It seems best as a general plan to introduce this and the following sections with a general historical summary (condensed as briefly as possible) and then to add special chapters on those sides of the period under review which demand detailed treatment.

The principal event of this period was the coming of the first bombe - Agnus - in August 1940 followed quickly by two others. On March 17, 1941 Jumbo, the eponymous bombe of a new type, arrived after exhaustive trials at Letchworth and quickly proved its value.

With the bombe cribbery became more important, though cillies were for long a valuable line of attack especially on new keys. However, the Crib Room was set up as a separate entity on October 1, 1940 and rapidly developed and expanded.

While Red remained the largest colour its size had dropped since the Battle of France and our growing resources enabled us to intercept more varied types of traffic. Thus more colours were broken and towards the end of this period two new keys - Brown and Light Blue - had joined Red in the category of regularly broken colours.

At the same time a number of other colours had been broken on several occasions, Blue, Green, Orange, Violet, A.F.5. (later to be called Chaffinch) and Onion. Most of these were broken at least in the first instance by the Research Section which in a very tentative way had its beginnings in the autumn of 1940. At this stage it had no permanent membership, and was simply composed of two or three people seconded from the routine shifts for a week or two at a time to work on the "odd colours".

It naturally happened that breaks of these new colours developed the theory of Rules of Keys, in particular in the case of Brown. Another development was the recognition of re-encodements between one key and another as an important subject of investigation and the first breaks on R.E.'s.

The immediate operational use of Hut 6 breaking in this period hinged on Brown - which in fact surpassed Red in urgency and importance. But no fewer than three of the new keys -- Brown, Light Blue and Chaffinch -- were closely connected with the current development of the war, as is made clear in the separate key histories later.

To conclude this summary, reference must be made to what was at the time an exciting, though somewhat mysterious development -- the breaking of Reflector C on cillies. Disquiet had been caused by some reference to a new reflector and its quick conquest was regarded as a triumph of [illegible] importance. Of two multi-teile messages on a Norwegian [illegible] 1180 one came out on the normal Red key while the other was dud: but the dud message provided some cillies to pronounceables, not exceptionally strong in themselves but very convincing in their agreement with the Red wheelorder. Moreover, cillies had occurred in the decoded message. So it was assumed that this obliging operatorhad enooded the first message with Reflector B and the later message on the new Reflector C: and it did not take long before C was broken on this assumption. The method adopted was that of rodding through each wheel in turn: as is pointed out in the technical volume the later invention of the half-enigma gave a quicker mechanical method of solving the problem.

Reflector-breaking became a commonplace in 1944: but the breaking of C has its unique place as the only time when it was possible to perform the operation on cillies. The practical results of the triumph were disappointingly meagre, as the Germans used Reflector C to such a small extent that the reason for its introduction remains most obscure. On Hut 6 traffic it was used for a few weeks only on its original frequency and then disappeared: its later use on some Naval keys does not fall within the confines of this history.

1.31 ARRIVAL OF THE BOMBE : WHAT IT DID

The bombe or spider* (Britain's secret weapon) is the most complicated piece of cryptographic machinery invented by Hut 6 with the possible exception of the reflector-breaking machines of 1944, all of which were to a greater or less extent modelled on it. In an earlier chapter of this book a sketch was given of the original conception of the bombe. What follows is thus to some extent recapitulatory, but it must be mentioned that the bombe as finally constructed differed in an important respect from the original conception. It was no longer necessary to construct a closed linkage and it was possible to use the principle of stecker implication to its full extent. How this was done is explained in the technical volume: in the present non-technical treatment of the subject it is desirable to attempt no more than to describe as briefly as possible what the bombe does without tackling the far more difficult subject of how it does it.

The material presented to the bombe is a menu - i.e. an equation consisting of a number of steckered constatations at known relative settings. These constatations can arise either from (1) a series of cillies with which may be combined a beginner or signature on a cillied message or (2) a crib, i.e. the plain text equivalent of part of an Enigma message.+

*Strictly speaking there is a technical distinction of some importance between these two terms: but the later term "spider" after being frequently used in autumn 1940 was superseded in common use by the earlier term "bombe", which will be generally employed in this work.

+ It is not possible to use two crib messages except in special cases (e.g. depth)

If the cilli or crib story is correct then there is at least one machine position (out of the $26^3 \times 60$ possible positions) where a consistent set of stecker can be found to satisfy the equation represented by the menu and to satisfy in addition all the constatations not used on the actual menu.

Now if we suppose that the correct position is known or at least reduced to such narrow limits that all possible positions can be tried by hand - as happens on a cilli story where there is a good ringstellung - then we can break the day by the stecker knock-out principle, i.e. by making up a menu and then trying all possible stecker pairings for one of the letters on the menu and following up the implications. As was said earlier, an initial wrong assumption is rejected on stecker contradictions: an initial correct assumption is verified by confirmations and self-stecker.

Now what the bombe does is to do just this on (if necessary) the full range of approximately one million positions. In every single position the bombe assumes all possible stecker pairings for one letter on the menu - known as the input - and works out the consequences of this initial assumption. Broadly speaking, the bombe stops at and records all positions that give possible answers, and the "stops" are tested by hand as described above. And the machine works so fast that it is able to run through an entire wheelorder in about a quarter of an hour.

Thus the bombe does over a vast range what any single person can do over a small range on an ordinary enigma machine. It is, of course, only able to act in this way because of its greater scale and complexity. Thus in a hand attempt it is customary to use only one Enigma which is set in turn at each of the positions required: but in the bombe we have a series of Enigmas which are set before the run starts at relative positions corresponding to the constatations on the menu and which travel in perfectly synchronised motion from one position to another.

The arrival of the bombes in August 1940 meant great changes in the organisation of Hut 6 which will be described in detail later. In the first place, it underlined the necessity of a study of the art of cribbery and a careful recording of all messages that might turn out to be cribs: hence the rise of the C.R. In the second place, there was a constant - and as time went on, increasing - demand for two types of work (a) making up of menus for the bombes (b) testing stops sent over from the bombes. The repairs and maintenance of the bombes were too technical matters to be entrusted to Hut 6 and were from the beginning in the capable hands of a staff of mechanics in a separate establishment: the actual running of the machines was done by trained Wrens.

The making up of menus - a more complicated affair in some ways at first than it was later - was the business of the Machine Room and so at this period was the testing of stops. As time went on this last task became so heavy that a separate section of the Hut was set up as a Testing Room to do this work. Historically this room was a descendant of the old Netz Room and carried on the name (although it was now meaningless) until 1943 when on the formation of Watch and Research as the main cryptographic sections the N.R. became known as the M.R. or Machine Room: a far more appropriate title as by then practically all the normal testing work was done by the girls of the M.R.

and consequently they possessed most of the Enigma machines used in Hut 6.

1·32 THE ESTABLISHMENT OF THE CRIB ROOM

The breaking of the Enigma on cribs had been considered as an academic question from the earliest days: but with the arrival of the bombe the problem assumed the most vital importance, for any key could now be broken if 20 - 40 letters of the text of any one message could be correctly guessed.

On October 1, 1940, the Crib Room was formed, consisting of four men who had previously been engaged in registration, under the leadership of Mr. Milner-Barry, who had been studying the cribbery problem. At this time cillying was still common and there were only two bombes; constantly, therefore, problems of priority on the bombe arose. Should a 60% crib on Brown start running on 60 wheelorders early in the day when there was also ready a 90% shot on Red and cillies would probably later reduce the Brown wheelorder? In general the answer was that cribs were run where possible on cilli wheelorders, and were only run on all wheelorders if they were thought certainly correct. So then the circumstances demanded a very high percentage of accurate guesswork from a section totally without experience in the work; and the successes achieved right from the beginning were a remarkable tribute to the energy and ingenuity of its members.

Methods improved as time went on, but the beginnings of most of the elaborate Watch technique of later years can be seen in the early days of the Crib Room. Routine messages were spotted from the typed books and, if good enough, details of their form and identification marks were entered in folders. To quote from a note on the work of the Crib Room written in May 1941, "Likely looking messages are usually identifiable by a combination of length, frequency, time of origin, time of intercept, callsign, whether KR etc. --. The actual analysis is performed by trying all known variants and if possible, thinking of forms which might have occurred but have not done so. Finally the crib is graded A, B, or C according to whether it permits e.g.,

Only one favourite form;
Two or more favourite forms, etc..etc."

Thus crib records were highly organised from the first, but the most satisfactory method of keeping them up to date was not brought in until long afterwards. In the early days the traffic was sent through after decoding to Hut 3, and later returned for the entry of cribs: this frequently resulted in delay in the observation of new cribs and new forms of old ones. Hence the system of K.P.'ing (entering en passant) was introduced, whereby each message was inspected by a member of the Crib Room before being sent through to Hut 3. But this was not till much later; in the early days the Crib Room Log, which was from the beginning used to pass on information from one shift to another, contains many references to the non-entry of cribs, and the difficulty of recovering the messages once the intelligence people had begun to work on them.

Exploitation of re-encodements was until 1942 in a rather primitive stage. The 1941 account quoted above says "Occasionally profitable are exact or almost exact re-encodements from one colour to another, e.g. Red to Light Blue or Brown". Methods of using R.E.'s when the texts were not letter-for-letter the

same had yet to be discovered by sheer necessity in the Chaffinch era. Meanwhile the art of cribbery was steadily developed, the members of the section becoming gradually surer in their touch as they gained experience which was to be the foundation-stone of the later successes of the Hut.

1.33 NEW DISCOVERIES ON RULES OF KEYS: BROWN

During the period under review the most important discoveries in the sphere of Rules of Keys were concerned with Brown. This unique key is in many respects unquestionably the most interesting of all keys broken by Hut 6; and its initial break was one of the greatest sensations of Hut 6 history. Brown is treated from a more general standpoint later: here we confine ourselves to its key pecularities.

Brown was first broken on cillies on September 2, 1940, and the key had six pairs of stecker and 14 self-steckered letters. This was the first known occurrence of a 1940 key with fewer than 10 stecker but that this was no isolated fluke was proved by the subsequent Brown breaks which all revealed six or seven stecker pairs. This peculiarity put Brown in a class by itself, at least so far as the then known keys were concerned; it will be remembered, however, that all the 1939 keys broken had fewer than ten stecker, and it is natural to consider Brown in this respect as the last survivor of an older order. It was quite clear from later discoveries that the Brown keys were not made up in the central G.A.F. Cipher Office and we tended to picture the Brown keymaker as the doyen and diehard Tory of his class.

As soon as a sufficient number of Brown keys were available for examination we looked to see whether the Red key rules were observed. It was at once clear that Brown obeyed none of these rules - not even that against repeats of stecker pairings within a month, though with the limited number of stecker this rule would have been easy to keep.

But in December 1940 an important discovery was made. It was noticed that since October 15, 1940 Brown had been pairing its stecker - i.e. in every pair of days one day had six stecker pairs, another seven and between them the steckered letters accounted for every letter of the alphabet. This meant that if one of the pair days were out 12 or 14 self-steckered letters were known on the next day; e.g. on October 15th the Brown stecker was A/F I/V J/U M/T O/S P/X R/Y and on October 16th B/K C/E D/G H/Z L/W N/Q. Unlike some key discoveries, this was of immediate and vital importance for breaking: for not only were the chances of hand breaks - not inconsiderable in any case due to frequency of cillies, ringstellung tips and the half chance that any particular letter was self-steckered - immeasurably increased but apart from cillies altogether one might with half the stecker known break "on the rods". (See the chapter on Rodding in the technical book.) This latter possibility was exploited at once and within a few hours of the discovery of the rule December 12 Brown was out on the rods - the first break of any key in this way. A rush of rod breaks followed in the next few days and, generally speaking, in future it was only necessary to run Brown on the bombe one day in two at the most.

It was discovered from the way the rule worked that the Brown key month was not the calendar month but ran from the 15th of one month to the 14th of the next. Hence whenever the month

consisted of 31 days the 14th was an odd day. It also follows from this that the Brown keys must have been made up for the particular month in which they were used otherwise the pairing would not have fitted in for such a month as February 15th - March 14th 1941. This is opposed to the general practice of the G.A.F. Cipher Office, where it is clear that keys were made up for a "standard month" of 31 days so that they could be readily transferred from month to month if this were desirable.

The pairing rule did not hold before October 15 - though there is a rough approximation to it on October 11 - 12, 13 - 14. It did hold consistently from October 15, 1940 to May 14, 1941, during which time Brown was broken almost daily. There were very few excentions to the strict rule in this period - once or twice there were slight slips which may have been due to a typist's error in copying out the original keymaker's script: they all consist of one letter being steckered in both keys and consequently one being unsteckered on both pair days. Apart from this the only oddity is that on March 15 and 16 1941 there were only six stecker pairs, F and Z being unsteckered on both days.

After May 14 Brown repeated back keys for ten days and this was followed by a period when little Brown was broken. It appears, however, that the stecker pairing rule came to an end with the March-April key: at any rate it did not hold in the June breaks.

To conclude this chapter something should be said about how other keys were behaving. Red continued to observe the rules of June 1940 except that after December, the ringstellung was abandoned: while Light Blue (which began to be broken fairly regularly in March) behaved precisely like Red: non-clashing and non-repeating wheelorder, no consecutive stecker and avoidance of repeated stecker. Of the other keys broken - Blue, Green, Orange, Violet, Chaffinch and Onion - none was in sufficient quantity to warrant any far-reaching deductions.

The breaking of February 28th Light Blue was an important milestone in Hut 6 history in that after this time everyone expected a key to have ten stecker pairings. The discovery of the pecularities of Brown had thrown doubt on this, as there was no reason to believe that Brown was necessarily unique: and the fact that in the log of the period it is explicitly noticed that the Light Blue key had "ten stecker just like Red" betrays that no a priori assumption was made that this would be so. But when Light Blue had been broken the general opinion of the Hut seemed to regard the question as settled: we had then direct knowledge of seven keys, and six of these had used ten stecker from 1940 on. Henceforward Brown was put on one side as an exception: we would have been surprised to find another key like it and we never did.*

*It should be mentioned, however, that for a month or two in 1944 Llama, a home-made Sonderschlüssel used in Albania, had a large number of self-stecker.

1·34 THE ORIGINS OF RESEARCH

1·340 The Function of Research

Machine Room Research, or M.R.2, began in a very informal manner in autumn 1940 and gradually attained a more permanent and stable position. It was obviously desirable as soon as we became aware of the large number of keys that existed and felt ourselves in a position to devote some of our set resources to intercepting hitherto unbroken keys that a separate body of people should be entrusted with the specific task of trying to break the "odd colours" - as they were called to distinguish them from the current colours, Red and Brown, broken daily by the routine shifts in M.R. and C.R.

1·341 Early Organisation and Methods

At this stage, however, no permanent organisation was set up. The section had a variable membership, consisting of at most two to three persons at a time. In the great majority of cases they were seconded from the M.R. routine shifts for a week or a fortnight. Normally the researchers worked "permanent days". Their initial numbers were not sufficient for three shifts but in any case the type of work did not demand working a 24-hour day.

The methods adopted in tackling their problems were in essence the same as those used on routine shifts and previously described- the search for cillies, ringstellung tips and depths - except that the work was not done currently but several days late and that subtractions and the rest of the routine were not performed on the register but on the blist, i.e. a list of all messages on a key arranged not as the traffic came in but in German Time of Origin, which in most cases corresponded to the order of encoding. In these early days there were few blists to look at: and not unnaturally there was considerable competition for those which on past evidence were considered most hopeful. Still there was more work than might have been imagined: for the principal odd colour, Green, was well covered at this period and passed considerable quantities of traffic. It was the duty of the researchers to use every means they could devise for breaking the traffic and for that reason to acquaint themselves with whatever was known about the W/T background of the colours with which they were concerned; and at this period such information related mainly to Green. In fact, however, the finding of a cilli story was by far the most likely means of securing an initial break: too little was as yet known of the art of cribbery to expect correct guesses at what messages in an unknown key might say and with only two colours being broken regularly the day of re-encodements was not yet. It was thus natural that the researchers should be drawn from the M.R. and not as yet from the C.R. and in any case the C.R.'s limited membership did not permit the establishment of a research section now; but it should be said that if a break was secured the traffic was examined by the C.R. from the crib point of view.

1·342 Early Triumphs

The history of the more important groups of colours broken by Hut 6 is recounted in a later chapter which will contain many of the triumphs of Research, as for most of the war new keys were dealt with by Research in their initial stages; but the earliest

successes should be mentioned here to give a picture of the variety of the early work. If the researchers were fortunate enough to make considerable progress with a colour and its contents were sufficiently important to make current breaking desirable, the key would quickly be transferred to the routine shifts. This indeed happened with Light Blue, key of the C.A.F. in Africa, which was after several near misses broken on cillies in March 1941 and almost at once taken over as a current colour. Cillies, re-encodements from Red and cribs all combined to give Light Blue a flying start, and it is perhaps the classic case of the Research ideal - to break a new important key soon after its appearance and hand it over to the routine shifts as soon as possible. Shortly after a similar initial entry was made into A.F.S. (Chaffinch) on cillies but in this case full success had to wait for a later cilli break in September 1941.

But apart from Light Blue and Chaffinch the researchers had two major triumphs in this period. The first was the breaking of November 19 Green on a hand attempt: by the rarest of lapses on this most secure of keys there was a keyboard cilli story and a good ringstellung. The second important break was an entry into Orange December 10 on a nearness story - a break secured on the memorable December 12, the same day on which the Brown stecker pairing rule was discovered.

This Orange day was the first war-time break of a new class of keys - the S.S. keys - which will receive detailed treatment later. In this case it proved possible to exploit the initial break and four days were broken in January 1941 on a crib called Fehlanzeige - the first crib to secure any regular success on a Research key. But the early disappearance of this crib left us nothing to work on but cilli stories - which were, indeed, available at not too long intervals but had the annoying habit of being rather sketchy and insufficient. For a considerable period, indeed, Orange was a tantalising colour, raising one's hopes only to cast them down: it was possible to try quite a number of days - sometimes on laborious hand attempts - but to break very few. For example, in the four months from February to May 1941 only one break was achieved - March 22nd by hand.

Green (or Greenshank, as it was later called) proved much less easy to exploit. Two methods were tried at the time and also much later: one was running the address AN STELLN GEN KDO ROEM in some form or other on suitable messages; but this, though with some support from the day broken, was failed ad nauseam. The second line of attack was the famous Banburismus method. This is the only way of breaking an Enigma key that does not presuppose the ability of writing out the clear equivalent of cipher text but its utility is severely restricted by the unfortunate fact that it postulates a great quantity of traffic - probably at least 400 messages. So Green - apart from, of course, Red which could be and was broken on more normal means - was the only Hut 6 key that could be attacked by Banburismus; but the most pertinacious attacks failed.* It was in fact not till March 1942 that Greenshank was broken again, and November 19, 1940, had at least the distinction of being pored over years after as the latest available evidence.

*Banburismus was often used successfully by Hut 8 and a full description of the method as applied to Naval problems will be found in the technical volume.

1.343 Summary

This brief account of the early work of M.R. Research may serve to show the general place that Research - which of course, came to include the crib side also - played in Hut 6. Research was the pioneer cryptographic section, breaking new ground and extending the frontiers of what was known. It was not always true that new keys were treated by Research in their first days; later, keys closely connected with existing Watch keys would be treated currently from their first appearance. Still, by and large, new keys were the province of Research. It inevitably happened that, the more successful Research was, the more was its own sphere of work limited; the area of the unknown grew less and less. And in the end, as we shall see later, Research died as a separate organisation largely in virtue of its own successes; but this self-immolation is a measure of its triumph. Broadly speaking, at the end so much was known that there were no more cryptographic worlds to conquer.

CHAPTER 1.4

PERIOD IV: JUNE 1941 - DECEMBER 1943: WORLD WAR:

THE GREAT PERIOD OF EXPANSION AND CONSOLIDATION

1.40 GENERAL HISTORICAL SUMMARY

1.400 Features of the Period

This long period of over 2½ years is not the time when Hut 6 reached the peak of its success if success is to be measured by the quantity and quality of the intelligence sent to Hut 3: on those standards the peak is in the last period of the war, probably especially in the months immediately following D Day. Yet the period now under consideration is the great central epoch in Hut 6 history, the time when thanks to increase of resources all round - sets, personnel and bombes - we got so completely on top of the enemy's cipher system (especially on the Air side) that all the ingenuity of his subsequent innovations failed to shake off our grip. At the end of this period Hut 6 could claim that practically every key which was passing a large amount of traffic (Greenshank was the most notable exception) was being broken with at least fair frequency and that a satisfactory solution had been found to every technical problem with which the enemy had so far confronted us. The salient features of the period are the great increase in the number of keys recognised, named and broken, corresponding increases in our personnel and machine strength combined with a growing complexity in our administrative arrangements, great developments in the regular technique of breaking, the frequent use of several new methods made possible by G.A.F. key repeats, a much greater concentration of attack than before on the not immediately operational keys so far as this could be done without detriment to those of operational value, and improved liaison with Sixta and Hut 3. It willbe convenient now to devote a paragraph to the above tendencies which will serve as an introduction to more detailed treatment later where this is desirable.

1.401 Increase of Keys

A certain proportion of this may be fictitious and represent merely the discovery by our greater interception resources of keys that were in use already; but when full allowance is made for this factor there can be no doubt that there was a vast increase in the number of keys issued and used by the enemy. For this there were two main reasons: (a) the initiation of new campaigns by the Germans or their preparations to meet expected attacks by the Allies and (b) the splitting up of keys by the Germans themselves because of alterations in their system of key distribution and allocation. Examples of (a) were the appearance of Mustard, Vulture, and Kestrel in June and July 1941 immediately after the attack on Russia and on the other hand the appearance of Albatross and Cormorant in May 1943 in anticipation of our attacks on Sicily and Italy. Examples of (b) were on a small scale the break-up of Kestrel into several geographically distinct keys in August 1941 and the similar disintegration of Raven in December 1943 and on a larger scale the complete reorganisation of German key allocation in January 1942 when Fliegerkorps keys were carved out of Red. It should be noted in passing that matters sometimes worked the other way round: German changes in key distribution might occasionally lead to the disappearance of a key (as Light Blue died in January 1942) while the same effect might be attained on the conclusion of a campaign - the most conspicuous instance of this was the unlamented death of Phoenix and the Finches in the Cape Bon peninsula. But for this period such cases were exceptional: for German keys the forces of new creation and fission were still stronger than those of death and amalgamation.

1.402 Increase of Personnel

The new fields opened up demanded staff increases in every section of the Hut. The main cryptographic sections (Watch and Research in the latest terminology) were considerably expanded not only by new arrivals from outside but also by recruitment from other sections of the Hut - especially the former Netz Room, now renamed the Machine Room. This section too was considerably strengthened to deal with the increased number of bombes and took over all the normal testing of bombe stops. In 1943 the constant influx of newcomers made it necessary for us to prepare a short course in cryptography and make other general educational arrangements which fall to be described later. In this year also began the American invasion, destined to add welcome fresh blood to the Watch, Research and many other sections of the Hut.

1.403 Increase of Machines

Along with the increase in personnel there was a considerable increase in our bombe resources: this was, indeed, a first priority in the eyes of those responsible for the administration of the Hut, and without their persistent clamour for more and more bombes Hut 6 simply could not have achieved anything like its actual success. The priority problems in this field were by no means straightforward as there were always the rival policies of concentrating on standard machines - i.e. aiming at mere quantity - and the more adventurous course of experimentation. Further, the requirements of Hut 6 and Hut 8, competitive users of the bombes, tended to differ. Experience taught us that you can scarcely have too many bombes: the more you have the more you use them up by embarking on long drives which you could never contemplate if you had not an apparent superabundance of resources. And thus despite the large number of bombes produced here Hut 6 would have suffered severely from insufficient mechanical resources - particularly in 1944 - had not the mass production of America come to our aid. Machine construction on a vast scale was in fact the peculiar contribution of America to Hut 6's success: in its full development the story belongs rather to the final period of the war but even in the latter half of 1943 we were already getting substantial aid both from the Military Bombe at Arlington and the Naval Bombes at Washington - witness especially the break of Bullfinch on a date stagger in December 1943, a form of attack which would have been inconceivable without American bombe resources.

1.404 Growing Complexity of Organisation

A natural consequence of the growth of work and of numbers was an increasing degree of specialisation in most sections and a growing complexity in the general organisation of the Hut. As far as the cryptographic side was concerned, this resulted (a) in Machine Room Research (or M.R. 2) being put on a more stable and continuous basis with a couple of permanent members assisted by a staff of visitors from the routine shifts and (b) in a corresponding Research section of the Crib Room being set up under the name of C.R. 2. We now had two pairs of sections - M.R. 1 and C.R. 1, M.R. 2 and C.R. 2 - each pair dealing with the same material from a somewhat different standpoint. It was realised that, however naturally this division had arisen, it was wrong in principle and persistent attempts were made to correct the error and arrive at a closer integration of cryptographic effort. Eventually, when the ground had been carefully prepared M.R. 1 and C.R. 1 were formally united as the Watch, while M.R. 2

and C.R. 2 were also amalgamated as the Research Section, and at the same time their membership was set on a permanent basis. These important developments (which coincided with the abandonment of the old Hut and our move to the newly-constructed Block D) are fully discussed later.

1.405 Technical Developments

These fall under three main heads (a) cribbery, (b) re-encodements and (c) new methods of breaking. In all cases full details are to be found in the technical volume.

The theory of cribbery can fairly be said to have reached its final development by the end of 1943: afterwards it was mainly a matter of employing known principles. Our experience in 1941 - 1943 made us familiar with all the different types of messages, and through this experience we became able on occasions to guess cribs on the slenderest of evidence. The important Army distinction between ordinary and Staff keys was first apparent from our observation of Chaffinch decodes in 1941 and 1942.

While re-encodements were first used successfully in March 1941 it was not until the present period - and particularly not until the great extension of keys in January 1942 - that they really came into their own. In anticipation of this multiplication of keys a mechanical means of discovering potential re-encodements (soon to be known as "kissing") was instituted on Air keys in December 1941 and at a later date the method was applied to Army keys also. The technique of working re-encodements underwent a great development and on the African Army keys in particular a chain of re-encodements became the recognised method of exploiting an initial break. Experience was also gained in what is often a most difficult task - working a re-encodement to Enigma from some other cipher (e.g. Fish): the peculiar trouble in such cases is to make adequate allowance for changes in punctuation.

The new methods of breaking came into their own in 1942 through the remarkable series of G.A.F. key repeats to be described in a later section. These made it possible on occasion to break a key (1) by rodding, (2) by running a hoppity menu on the bombe or (3) by the dottery method. The last two of these were new methods: (2) had not been used in Hut 6 practice until 1942 (though it had been employed by Hut 8, and hence the mechanical device was ready for use) and (3), though developed in theory in autumn 1941 and once used in Hut 6 practice, did not come into its own till 1942.

Apart from these strictly technical developments fresh discoveries in the Rules of Keys - particularly as regards G.A.F. wheelorders - increased the number of breaks by saving bombe time: and the curious story of the HOR-HJG stecker on Orange (see the section on S.S. keys) led to a new kind of rodding - rodding with half the stecker known. This, it is true, was not in principle different from rodding Brown on known self-steckered letters, but in practice was somewhat harder.

1.406 General Course of Breaking

Throughout the whole period supreme emphasis was placed on the Mediterranean keys - on the Air side Red, Primrose, Locust, Scorpion II and later Puma; on the Army side Phoenix and the Finches up to May 1943 and later Albatross, Cormorant and Shrike: but as far as possible without detriment to this priority we

attempted to break anything in sight. On the Air side we succeeded in breaking many Luftgau and Fliegerkorps keys, including some on the Eastern Front, also large quantities of Mustard, the G.A.F. Y key, and of the Weather keys more than enough to satisfy all intelligence claims: on the Army side we made increasingly successful inroads into the Balkans and tried to break Vulture on every opportunity, though we could seldom get any long sequence of breaks; we scored sporadic successes also on Kite, Osprey, Robin, Gannet and a few other keys. Of the S.S. keys Orange and Quince were both broken frequently and in the case of Orange cheaply so long as the HCR-HUG stecker lasted. It should be noted that (especially in 1942) the key repeat system made it more than ever absurd to organise our Air breaking on a basis of intelligence priorities alone: for no one could tell whether a key of negligible intelligence value in one month might not prove to be of the highest cryptographic value in helping to break an important operational key the next month. In the G.A.F. key world everything was so interwoven and interlocked that the only safe rule was to try to be in a position to break any key on demand even if one did not have the resources to do so regularly: if this ideal was achieved then we could take full advantage of any key repeats that were discovered and also be reasonably certain of not missing any discoveries. As a step in the latter direction it was a definite point of policy to have an exceptionally vigorous drive on the 1st of every month and to attempt to break on that day every identifiable key, no matter how trivial might be its content.

1.407 Liaison with Sixta

During this period liaison with Sixta - the organisation responsible for log reading and "fusing" together all information of W/T interest - became closer than formerly, though not yet so intimate as in the last period of the war. But even at this stage liaison with Sixta was invaluable for securing to Hut 6 up-to-date information on all W/T matters that might affect cryptography. Sixta's special responsibilities were (a) working out new W/T systems by evidence of logs, callsigns, direction-finding, etc.; (b) discovering re-encodements by charting, log reading and other methods; (c) answering specific enquiries about routeing of messages, indicators etc., and (d) bringing to the notice of the cryptographers any significant log chat. No official liaison body was ever set up between Hut 6 and Sixta: contact was maintained by day-to-day intercourse between the parties concerned, who were in most cases the Fusion Room officers on behalf of Sixta and members of the Crib Room or Machine Room (later Watch and Research) on behalf of Hut 6.

1.408 Liaison with Hut 3

The importance of liaison with Hut 3 was that only in this way could Hut 6 receive adequate guidance as to the intelligence priority of various colours i.e. which colours were most important and most urgent to break. (The two categories did not necessarily coincide. Of course, final decisions could not be made on intelligence values alone: Hut 6 had to weigh these in the light of cryptographic probabilities, otherwise we might have gone on failing poor shots on important colours while good shots on less important colours waited. But it was at least essential that Hut 6 should know as accurately as possible what the intelligence priorities were; and this information could only be supplied from Hut 3. So inevitably from the earliest days an informal liaison grew up, and in 1942 this had progressed so far

that in some instance advance information of war moves was passed on to the senior members of Hut 6 so that they could if necessary reconsider their breaking policy. But at this stage the need was felt for a more regular link and a separate section (known as 3L) was set up in Hut 3, one of whose functions was liaison with Hut 6. Henceforward (except in emergencies) all advice on intelligence priorities (for breaking and decoding alike) came to Hut 6 from Hut 3 through 3L and it was one of the functions of the Head of Hut 6 to keep in constant touch via 3L with the general intelligence background.

After the formation of Watch and Research the liaison with 3L became still more formal and official. In July 1943 a daily meeting (taking place normally at 5 p.m.) had been arranged between officers of the Watch with the Head of the Research Section and the Head of the Hut to discuss the bombe programme for the next 24 hours. (This meeting was required because the very length of the Research programme to be run on the bombes made a clear system of grading necessary). In September 1943 this meeting, known as the Lage Conference, was extended to include a representative of 3L. At this conference the general cryptographic situation (including the bombe resources available) was set forth by representatives of Watch and Research; the general intelligence situation was explained by 3L and finally after any questions from either side the lage - i.e. the list of jobs to be run - was arranged in an order of priority that struck a fair balance between the claims of Intelligence and Cryptography. The Lage Conference remained as a useful piece of machinery till the very end of the war: its final form is discussed in the section on the Organisation of the Watch.

1'409 Conclusion

It may be useful to add here a brief list of some of the important dates of this period, including the first breaking dates of the more famous new colours.

June	1941	First breaks of Vulture and Mustard
August	1941	First break on the dottery
September	1941	Beginning of regular breaks of Chaffinch
December	1941	Beginning of regular breaks of Vulture
April	1942	Discovery of HOR-HUG stecker
April	1942	Discovery of G.A.F. key repeats
May	1942	Greenshank of March 5th broken
June	1942	First break of Phoenix
August	1942	New record of 508 breaks in one month
October	1942	New record of 555 breaks in one month
December	1942	First use of wahlworts i.e. nonsense words affixed to the beginning and end of messages
June	1943	First break of Albatross
October	1943	First break of Wryneck
December	1943	First break of Bullfinch

It should also be mentioned here that during this period the Germans adopted various security measures. The most widespread change of this nature was the permutation of wheelorder, finally adopted universally in some form or other. This was clearly an anti-depth device and from this angle fell in the same category as later further security measures (e.g. Uhr stecker and Enigma Uhr). [illegible] to a considerable extent [illegible] but [illegible]

out the banburismus method as a practical one for Hut 6 and certainly ensured the failure of the banbury attempts on Greenshank in 1942 as on this key the alteration of wheelorder was particularly thorough.

The first step in wheelorder change (so far as we knew) was taken by the G.A.F. in October 1941 when Red and all other Air keys (except Brown, which as usual came into line later) adopted the system of A.M. and P.M. wheelorders - i.e. at 12 noon the wheels in the machine were taken out and simply reversed, this also reversing the ringstellung. The German Time of Origin of any message determined whether the A.M. or P.M. wheelorder would be used.

In July 1942 a more radical change was made on all pure Army keys. Three wheelorders were used daily from 0000 - 0759, 0800 - 1559, 1600 - 2359 respectively, the permutation being cyclic - ABC, CAB, BCA. (At a later date when the key day began at 0300 all the times were put three hours on.) In September 1942 the G.A.F. came into line (Brown as usual lagging), as also did Orange, then the principal S.S. key: by December 1942 Quince had also adopted the system of X, Y, Z wheelorders as they were called. The system was indeed by now virtually universal: it should be stated that the wheelorder first used on any day (i.e. the A.M. or X wheelorder) was the basic one printed on the key-sheets and as such the relevant wheelorder for key rules.

Two Army keys (Greenshank and Nuthatch) were found to use a different system. Both employed all six permutations of a basic wheelorder, the order of the changes being variable and decided by a daily changing table. The times of alteration were irregular - on Nuthatch when the key day started at midnight they were 0000 -1115, 1115 -1330, 1330 -1500, 1500 -1700, 1700 - 1800, 1800 - 2400. The basic wheelorder - which was presumably written on the key-sheet - was that with the wheels in ascending numerical order and not necessarily the first wheelorder of the day. Further details of the wheelorder peculiarities of these keys will be found in the section "Greenshank and Allied Keys".

More isolated security measures such as the ringstellung peculiarities of Orange and Mustard are dealt with in the special key histories while the W/T camouflage measures at the end of 1943 - viz. the dropping of discriminants on Army keys in September and on Air keys in November - are discussed in the Book on Traffic Identification.

1·41 DETAILED THEORY OF RULES OF KEYS

1·410 Sources of Information

With the large number of breaks in this period our general knowledge of the workings of the German cipher system greatly increased and it became possible to treat rules of keys in a more systematic manner. The principal source of our deductions and conclusions remained the actual keys broken in Hut 6: but a subsidiary source of value was the examination of captured keys and documents. True it was not until the summer of 1944 that these began to arrive in Hut 6 in large quantities, but at least one important point was confirmed by captured documents as early as 1941.

1·411 Air and Army

The fundamental distinction of Air and Army keys first became clear in 1942. These two types of keys were found in general to obey so divergent rules that it was obvious that the G.A.F. cipher office was distinct from the Army cipher office or offices. This was most clearly shown by the remarkable key repeat system on the G.A.F. which reached its climax in 1942: this system to which the relatively few Army repeats provide no real analogy is dealt with fully in the next section. The divergence is also suggested by the fact that the G.A.F. and Army used different discriminant books; for to the Germans the discriminants (which appeared on the key-sheets) were an integral part of the key. Thus in considering key rules it is necessary to make a sharp distinction between Air and Army keys. In our conventional key nomenclature Army keys were given bird names, while Air keys were called after colours, insects, flowers or various types of animals.

The S.S. keys (fruit names) are in the wide sense Army keys, but had to some extent peculiar key rules, and were possibly made up by a separate S.S. cipher office. Indeed it was never quite clear whether all the "pure Army keys" (i.e. Army keys excluding the S.S. keys) were constructed in the one office or not. In the case of Air keys it is clear that they were all constructed in a central office except for Brown (which was always in a category of its own) and a few locally issued special keys.

1·412 Divisions of the Subject

The theory divides naturally into four parts which will be dealt with in the following sub-sections. These divisions are (1) wheelorder rules; (2) ringstellung rules; (3) stecker rules; (4) Brown rules.

1·413 Wheelorder Rules: Army and Air

On Army keys wheelorder rules were conspicuous by their absence. Even the fundamental Air rules of non-clashing and non-repeating wheelorders were frequently broken by the Army and the S.S.: in fact, the incidence of clashing wheelorders in this period was as a rule not less than random, and sometimes one could almost have given a preference for the clash.

On Air keys on the other hand (excluding Brown -- this is to be understood from now on) these rules were observed with very few exceptions and in themselves gave helpful wheelorder reductions. At various times, however, other more precise rules were discovered and these now fall to be described.

(1) The Clarkian Wheelorder Rule This rule held on Red and Light Blue from August to November 1941 and was named after its discoverer, L.E.Clarke. To follow the subsequent discussions the reader should refer to the Table of Wheelorders which is inserted here.

The rule states that in the same column no wheel is followed by a consecutive wheel: 5 and 1 are not, however, regarded as consecutive. It will be noticed that there are only some half-dozen breaches of this rule in the four months. Its effect is, of course, supplementary to the normal non-clashing and non-repeating rules and the conjunction has a powerful effect in reducing wheel-orders -- in general (apart from the non-repeating rule) four to ten legal wheelorders are left. It is also usually possible to reduce a Clarkian sandwich to a single wheelorder: see examples of this in the Table.

Before August 1941 the rule is not very noticeable though there are no actual contradictions in Light Blue of July: but in view of the numerous gaps in that month and the bad record of Red, it is very doubtful if the rule really held then. In December it broke down definitely on Red, though on Light Blue a preference for Clarkian wheelorders was even yet worth while: but the demise of Light Blue at the end of December meant the end of the rule.

Before leaving this subject it ought to be mentioned that with the Clarkian rule there was a tendency for wheelorders to run in cycles -- at least two well-marked cycles of eight appeared. (These are marked A and B on the Table.) This phenomenon naturally made prediction of the day's wheelorder a popular parlour game in the Machine Room and attempts were made to discover a deeper system in the sequence of wheelorders within a month. However, as in the later case of the Nigelian wheelorders, all such attempts proved abortive.

TABLE OF CLARKIAN WHEELORDERS -- AUGUST TO NOVEMBER 1941

Day	Red					Light Blue			
1	154	235	425		421	123	(231	253
2	431	451			153	451	(453	521
3	253	124	531		325	134 B	(125	145
4	425	351	124		541	312	(341	312
5	142	135	352			154	(513	154
6	325	452	524			431	(235	432
7	153	214	241	412	125	254	(542	215
8	524	531	513	135		512		543
9	342	243	135			435	351	321
10	514	415	452	524	241	153	523	153
11	231	231	(215)			321	241	435
12	315	513	541	415		543		251
13	152	345	214	(231	412	125	132	524
14	324	521	345	(453	254	341	354	342
15	541	254	(512)	(125	531	513	521	514
16	213	532	134	B(341		135	(254)	(231
17	435	315	351	(513		352	421	(453
18		143	523	(235	524	514	253	(125
19		421	245	(452		241	435	B(341
20	542	253	321	(124		423	152	(513
21	314	435	154	541	521	251	315	(235
22	531	152	412	213		534	543	(452
23	215	(321	543	435		152	(321	(124
24	452	(145	315	153		325	(145	351
25	124	(423	132	(321	215	143	(423	135
26	341	A(251	514	(145		415	A(251	
27	513	(534	342	A(423	514	231	(534	
28	235	(312	(125)	(251		413	(312	
29	451	(154	453	(534		145	(154	
30	134	(431	231	(312	341	421	(431	
31	352	---	415	---	513	---	215	---

In the above table A and B represent the two long cycles of wheelorders referred to.

Wheelorders enclosed in brackets are not known from breaks, but are the only legal Clarkian ones.

Breaches of the Clarkian rule are indicated by underlining the offending wheels.

It may be worth mentioning the Clarkian sequences which are:-

1; 3,4 or 5; not 4
2; 4 or 5; 1,2 or 3; not 2
3; 1 or 5
4; 1 or 2; 3,4 or 5; not 4
5; 1,2 or 3; not 2

(2) The Nigelian Wheelorder Rule This second and far more important rule lasted on the majority of Air keys for just two years -- i.e. May 1943 to the end of the war. Like the Clarkian rule, it was a supplement to the ordinary non-clashing and non-repeating conditions. It stated that all Air keys selected their wheelorders not from the complete list of 60 but from a list of 30, known as Nigelian after the discoverer, Nigel Forward. This discovery had naturally a tremendous effect in reducing the number of bombe hours per menu, especially towards the end of a month. The obvious difficulty that all keys had to be made out for a 31-day month (to allow for transferences in the event of compromises) was got over by a relaxation of the rule for the first five days on any month: on these days a repeated or non-Nigelian wheelorder was permissible. (Actually the 1st and 2nd were the dangerous days: the 3rd, 4th and 5th days have records only a little worse than days after the 5th.) In practice, therefore, up to the 5th we ran on the normal legal wheelorders with a preference only for Nigelians: after the 5th we gave preference for Nigelians and excluded wheelorders used since the 5th: and as soon as it was considered safe to declare the key Nigelian we ran on Nigelian non-clashing non-repeating (since the 5th) only. How soon the final declaration was made depended on the importance of the key and the strength of the cribs normally available: at the beginning of each month general principles were laid down for the more important keys. And, of course, as even the best established wheelorder rules were sometimes broken, it was always open to the Air Head of Shift on sufficient reason to run any particular crib on illegal wheelorders.

TABLE OF NIGELIAN WHEELORDERS

132	235	312	342	421	514
142	241	314	345	425	523
145	243	321	354	432	524
152	245	325	413	512	531
153	251	341	415	513	534

The discovery of the Nigelian wheelorders gave rise to an interesting problem. Was the selection purely random or dictated by some system? The very peculiarity of the rule and in particular the fact that there are only 30 and not the convenient 31 Nigelian wheelorders suggested the probability of a system, but the list of wheelorders (given above in the order usually adopted for writing out) seemed at first sight quite arbitrary. However, closer examination reveals that each wheel occurs precisely 18 times and this suggests that one object of the rule was to level out the incidence of occurrence of the several wheels and thus avoid any unintentional favouritism of a particular wheel.

A still more detailed analysis discloses that the wheelorders fall into ten triads, each triad consisting of three out of the six possible permutations of any selection of wheels. This certainly looks like intention, and explains how the figure of 30 is arrived at. But it is unfortunately impossible to reduce each triad to the same pattern. If to secure standardisation we arrange each triad so that a wheelorder reads down and across in the first, second or third row and column, and that we also have a "diagonal" from top left to bottom right, we have six triads of the pattern

ABC
BAC
CBA,

three of the pattern ABC
BAC
BCA,

and one of the pattern ABC
CAB
CBA.

The basic Nigelian wheelorder -- i.e. ABC in the above patterns -- are 132, 152, 153, 241, 325, 342, 413, 415, 425 and 534 with each wheel occurring twice in the second position. It does not seem possible to carry any further the analysis of the Nigelian list and no system was ever discovered by which the permutations into monthly key blocks were arranged.

(3) The Monrovian Wheelorder Rule It should be mentioned that apart from Brown and the local keys such as Yak, Llama, Raccoon etc. which were never Nigelian) there was in some months a non-Nigelian minority of Air keys. Some of these keys (but by no means all) were found to obey the Monrovian law, named after its discoverer, Major Monroe. By this rule the five wheels were all used on any two consecutive days in the month -- it will be seen that a Monrovian wheelorder, like a Clarkian, is a purely relative conception. This rule was never so absolute as the Nigelian and it is usual to find one or two exceptions even on keys where it is generally held; nor was it ever very widespread. Till the end of 1943 Monrovian keys were October Primrose, November Primrose, Squirrel and Cookroach and December Leek, Puma, Hornet and probably Beetle.

(4) Tricycle Keys To conclude this subject of wheelorder we should mention one interesting, if completely unimportant, survival. In 1941 and 1942 we broke several days of "Tricycle" as it was called, a type of traffic that used the old outmoded indicating system of enooding the message setting twice at a fixed Grundstellung. All the days broken used a permutation of the wheelorder 123, and it was suggested that Tricycle only used these three wheels: hence, indeed, the name. While this hypothesis was hardly decisively proved (as owing to lack of traffic and its low intelligence priority we were able to secure very few breaks) it is not so fantastic as appears at first sight; for it is known that wheels 4 and 5 were later additions to the Enigma machine, and it is not unreasonable to suppose that a key which was still in 1942 using the obsolete indicating system described above might still keep to the original six wheelorders. The traffic was Abwehr in content and not directly connected with the German armed forces, and even in 1942 there was no wheelorder permutation in the course of the day.

1·414 Setting up of Committee on Rules of Keys

The discovery of the Nigelian wheelorder rule in August 1943 had an important consequence. It may have been noticed that rules were often not discovered till several weeks or months after they had come into force: this is to some extent inevitable, as a new rule cannot be discovered till there is a sufficient body of evidence to make the necessary deductions. However, it was now clear that the problem of discovering key rules at the earliest possible moment must be taken up more thoroughly than before and not left merely to private enterprise. Consequently a small committee was set up to issue reports on such questions at suitable intervals and strenuous and sucessful attempts were made to induce parents of keys to write out each month's keys on a key-sheet*

* The key-sheet system (which, of course, corresponded to the German layout) had been first introduced in 1942, but had somewhat lapsed till it was generally revived in September 1943. The system of key parentage is discussed later in Section 1·43.

in a form which was more suitable for analysis of rules than the daily entries in keybooks. It is these records and reports that are the main authorities for the history of key rules since September 1943.

1·415 Ringstellung Rules: Army and Air

(1) The Army Ringstellung Rule It is again convenient to treat the Army first because of the relative lack of variety in its key rules.

In the autumn of 1941 during the British offensive in Libya a number of Army keys (viz. Chaffinch I, Chaffinch II, Phoenix and corresponding Reserve keys for November 1941 and Phoenix and Phoenix Reserve for December) were captured and sent back to us. These were closely examined (all the more so as they were the first captured key-sheets to be seen in Hut 6) and a ringstellung rule was quickly noticed. Every letter of the alphabet was used in blocks of eight or nine days: the exact divisions are to be seen in the example appended -- viz. the first five days form an odd set using up 15 letters of the alphabet, days 6 to 13 plus two letters from the 14th form a complete alphabet, the remaining letter of the 14th, one letter form the 23rd and all the intervening letters form a second alphabet and the rest of the month gives us a third. Occasionally there are slight errors in the system, and it should be noted that there are some variations in the method of splitting up the ringstellung letters on the 14th and 23rd -- see the following example for the orthodox method.

Immediately after the rule had been discovered it was confirmed by a captured document giving instructions for the use of the Enigma. In the course of hints for constructing emergency keys this document recommended that the letters of the alphabet be written out on small discs and that 24 of these be chosen to form the ringstellung of eight consecutive days -- a rudimentary version of the Army ringstellung rule.

The rule had previously been used on Yellow in 1940 and soon after its rediscovery in November 1941 it was found to hold on Vulture and also sometimes on Orange -- though never on any other S.S. key. However, until January 1944 when it disappeared the rule was observed by most Army keys[X] occasionally, though its observance could never be assumed in advance.

In general the rule was not a great deal of help in breaking except towards the end of a period: the colours on which it proved most useful were Phoenix and Orange where the occurrence of cillies and (in the case of Orange) the known HOR-HUG stecker made hand attempts possible if the ringstellung could be guessed.

TABLE: EXAMPLE OF THE ARMY RINGSTELLUNG RULE
(Phoenix, January 1943)

Day	Ringstellung
1	AZS
2	UDI
3	DRW
4	NTH
5	LBP

X The list included Yellow, Chaffinch, Phoenix, Vulture, Orange, Sparrow, Shrike, Bullfinch, Raven and Wryneck I.

TABLE: EXAMPLE OF THE ARMY RINGSTELLUNG RULE (Continued)
(Phoenix, January 1943)

Day	Ringstellung
6	SFJ
7	HAD
8	OBY
9	KVG
10	ZIQ
11	ETX
12	RLC
13	WAN
14	D)PU
15	LIS
16	NWB
17	YFQ
18	HKV
19	OTC
20	
21	JXE
22	MGP
23	WC(U
24	AQL
25	ZIS
26	OKG
27	VEX
28	MTM
29	RBP
30	NJD
31	YFU

(2) Air Ringstellung Rules The Air keys at times observed ringstellung rules, but again these could not be counted on in advance. Many key-sheets show no rule at all in this respect, and each case had to be examined on its merits. It must also be remembered that for the period with which we are now dealing despite the high break figures there were still comparatively few complete months broken and Air ringstellung rules don't show up clearly unless a very large proportion of the month is out: the most regular colours were Red for the whole period and at intervals Locust and Primrose.

To the end of 1943 two main rules can be distinguished: (1) the old Red ringstellung rule used in 1940 and covering the first 26 days of the month and (2) the 31-day rule, an extension of the above by which all the letters of the alphabet were used in each ringstellung column, but the five repeats were irregularly distributed and not lumped together at the end. The first rule was the better from our point of view as the position of the repeat letters was fixed: but on the whole neither rule was of much assistance to breaking after 1940. Of course, it must be remembered that in 1942 all key rules were completely overshadowed by the key repeats which were fundamental to our whole breaking practice.

The 26-day rule ended on Red in December 1940 but revived in 1943 and was used on January and June Red, January, February and March Locust and April Primrose. The 31-day rule was so far as we can tell used principally by Red: but, of course, we have much more evidence for Red than for any other colour. It first appeared on Red in May 1942 and was used till August when it vanished till fleeting reappearances in February and July 1943. Once or twice

a curious intermediate rule occurred by which all the letters of the alphabet with one repeat were used in the first 27 days: examples are Red of February and March 1943, and Hedgehog of June. The above selection of facts may serve to show how variable and confusing is the whole subject: the numerous key-months not mentioned either show no rule at all or give insufficient evidence.

(3) Stuttering Ringstellung To conclude the ringstellung rules it should be mentioned that there was a marked prejudice against "stutterers" (i.e. ringstellung with a repeated letter). By chance these should be 11% of the whole but actually we can only collect 91 examples. Three of these are on Brown, one on Yak, fifteen on S.S. keys (mainly Orange) and the rest on Army keys with Falcon I and II principal offenders. It is noteworthy that all the examples except three appear in 1944 and 1945 and that there is no regular Air key in the list. One double stutterer occurred - GGG on Falcon I of December 8, 1944.

1·416 Stecker Rules: Air and Army

(1) Air Rules and Tendencies Here for once the Air rules are simpler and may be taken first. The rule against the use of consecutive stecker is one of the most absolute ever discovered. Brown, a few locally issued special keys and, of course, the NOT-keys of 1944-5 are exceptions: but of the many thousands of regular Air keys broken or captured only one (Mayfly, March 16, 1944) had a consecutive stecker; and the chance of any given ten-stecker key having a consecutive stecker is approximately $\frac{1}{2}$. This rule was one of the most consistently useful of all, as in running Air keys on the bombe C.S.K.O. could be and was regularly used.

The non-repeating stecker rule was also generally observed, though it was never again of such practical use in breaking as in the early days of hand attempts in 1940. More interesting was the fact that on most Air keys there was a constant tendency -- it can hardly be called a rule -- to diagonalisation [x] i.e. the use of stecker pairings which form a diagonal on a Foss sheet. An excellent example is the stecker of Primrose, July 22:

A/Y B/X C/W D/V E/U F/T G/S H/R I/Q M/Z,

where only the last pair is out of step: but there are many examples on other days of a smaller number of pairs on the same diagonal. If a particular key is noticed to be behaving like this frequently in a month, it is possible to try a still unchosen diagonal for the stecker of unbroken days, and on Primrose at least one triumph was achieved in this way. Again, it happened once that the right story was picked out on a dottery attempt by choosing diagonal stecker pairings: but obviously it is very seldom that one can bring off such tours de force.

From time to time persistent attempts were made to discover a complete system in the arranging of the G.A.F. monthly sets of stecker. It was not impossible or even one might have said unreasonable that the Cipher Office should have devised some means for reading off sets of stecker from a square or some similar figure so that as far as possible there would be no repeats in the month. But we were unable by analysis of keys to arrive at such a system: and we must perforce come to the conclusion that the German key-maker made up his sets of stecker on no other system except that -- possibly by setting out his stecker pairings on a Foss sheet as we

[x] How natural the tendency to diagonalisation is may be inferred from the fine example provided by the nomenclature of the Bletchley Park buses.

did -- he endeavoured by eye to avoid repeats.

(2) Army Rules in General and Particular Army keys never obeyed the Air law against consecutive stecker, though many keys had periods when consecutive stecker were very rare: still it was never possible without undue risk to use C.S.K.O. The S.S. keys on the other hand generally used consecutive stecker pairings to a more than random extent.

The captured Army key-sheets of 1941 did not reveal any helpful stecker rules. The pairings were not even written in alphabetical order except that the first letter in each pairing was the earlier in the alphabet. Otherwise the order seemed quite arbitrary except that in some keys there was a very rough and not very useful pattern in the first column -- a pattern (if we can call it so) which merely consisted in a progression in the alphabet of alternate initial letters or the like.

But, though there were no useful general rules, particular Army keys were always liable to throw up odd and ephemeral rules which were so confined in their application as to throw some doubt on the natural hypothesis that all Army keys were made up in a single central office like the Air keys. To the end of 1943 these Army stecker rules fell into two classes: (1) special stecker patterns and (2) stecker repeats within a month.

Under the first head must be cited the rule on Chaffinch II by which A and B were self-steckered on alternate days. The best example is July 1942 when out of 15 days broken A or B was self-steckered on 13, and in general the sequence was alternate. In September A or B or both were unsteckered on all 20 days broken, but the alternation was not well observed, and in October the rule (with exceptions and an increasing disregard of the alternate aspect) appeared on all the Chaffinches. There were also occasional signs of its appearance on Orange, but here the certainty of the HOR-HUG stecker made us prefer to ignore entirely this rather uncertain rule.

A more interesting and much more useful stecker pattern occurred on Albatross in July 1943. Most of the keys in this month showed the phenomenon known as "stepping stecker" i.e. stecker pairings all the same distance apart in the alphabet. Thus on July 1st the stecker ran

A/D E/H F/I G/K J/M L/O N/Q P/S T/W U/X

with a difference of 3 (G/K is of course an error): while on the 4th we had

A/G B/H C/I E/K J/P L/R O/U Q/J S/Y T/Z

with a difference of 6. It should be mentioned that addition does not carry over the end of the alphabet: hence it sometimes happens that the last stecker pairing is outside the system as on July 12 when we had

B/I C/J F/M H/O K/R L/S N/U P/W Q/X T/V

Fortunately in July the differences also were in sequence: we were able to break sufficient days to make it apparent that the full sequence must have been 34567XX 34567XXX 34567XXX 34567XXX, where X denotes a day without stepping stecker. Once this pattern

was realised we knew that on 20 days out of 31 every letter was either self-steckered or steckered to at most two definite other letters and it was possible to use this considerable stecker limitation on both hand attempts and bombe menus. It was particularly useful in making weakish oilli shots runnable: with cribs it was generally speaking unnecessary to run even the slight risk involved. In September 1943 stepping stecker again appeared on Albatross, but on this occasion the sequence of differences was too irregular for successful prediction.

Under the second head, repeats of stecker within a month, we must note the Balkan repeats in the autumn of 1943 -- an unprecedented phenomenon on Army keys. Raven of October 1943 was found to be repeating sets of stecker at intervals of 16 days apart; and in November the repeats continued at intervals of 14 days (thus stecker of November 1 = that of the 15th = that of the 29th). These repeats were exact, and as at this time the Raven crib position was as strong as it ever was, breaking on the rods was easy and rapid.

On Wryneck I, the other principal Balkan key, similar repeats were found to exist in October and December. In October the repeats occurred at slightly irregular intervals of 15 or 16 days: in December the 16 days interval was universal, days 17-31 repeating the stecker of days 1-15. The Wryneck repeats were not exact -- occasionally as many as three stecker pairings were altered -- but this disadvantage was offset by the greater strength of the Wryneck cribs and by repeats of the other key components. It was discovered that November Wryneck was the basic month: this was apparent from its observance of the Army ringstellung rule. The wheelorder and ringstellung of November Wryneck were used in different shuffled blocks in October and December, the ringstellung being sometimes permuted: the combination of all these factors meant that towards the end of December 1943 it was possible to predict the Wryneck wheelorder, the ringstellung letters and the approximate stecker. The result was that for a brief period Wryneck enjoyed the distinction of being broken currently in the Watch until the end of the repeats in January 1944 sent it back to the normal Research status of Balkan Army keys.

1·417 Brown Rules

Brown is best considered separately. Its special peculiarity is that at times the rules regarding wheelorder, ringstellung and stecker were so rigid that it was possible to attain the ideal of the investigator of key rules -- i.e. to generate a key from its predecessor and simply write the answer down.

In June after a long period of successful breaking Brown was virtually lost by one of the many temporary eclipses, mainly due to paucity of traffic, to which this colour was liable. When in December 1941 regular successes were again achieved, Brown was found to have split into two keys -- German and French, later known as Brown I and II. It is advisable to follow the career of these two keys separately, always remembering that the Brown key-month ran from the 15th of one month to the 14th of the next.

Brown I early developed the habit of choosing its self-steckered letters in a continuous or nearly continuous block: e.g. December 31, 1941 had O/P Q/R S/T U/V W/X Y/Z A/B with C to N inclusive self-steckered; and January 15, 1942 had A/N B/L C/K D/J E/I F/M G/H with O to Z inclusive self-steckered. This block rule was sometimes conjoined with the old stecker pairing

rule as e.g. on February 18 and 19 which had respectively B to O and P to A self-steckered and sometimes with a variety of the rule by which on both pair days we have a different set of self-stecker, but the whole alphabet is not used up: e.g. on January 15 and 16 the runs of self-steckered letters were from O to Z and then from C to N.

The tendency to blocks of self-stecker lasted till April, but the pairing rule continued much later and was in fact observed in most months up to June 1943 (November 15 - December 14, 1942 was an exception). Apart from the strict pairing rule -- viz. that all letters steckered one day are unsteckered the next, and that the steckered letters on the two days account for all the letters of the alphabet-- a modified rule was quite often employed by which the second regulation is waived. This relaxation suited the tendency to the frequent use of only <u>five</u> stecker pairs which arose in October 1942 and must be considered as a throwback to the sparing use of stecker in the pre-war days.

More interesting was the tendency to "universal stepping" which appeared occasionally on Brown I. However, the duration of this rule was always uncertain and it came up at irregular and unpredictable intervals. The first occasion it arose was on January 25, 1942 when there was a strong tendency to step on wheelorder, ringstellung and stecker with occasional deviations particularly in the case of wheelorder -- otherwise the wheelorders would repeat themselves after a cycle of five days. A few examples will indicate how the rule worked and it will be seen that it was sometimes possible to write the key down.

Jan.	25	452	MAI	A/B	O/Z	P/W	Q/X	R/V	S/T	U/Y
"	26	513	AOE	A/U	C/W	E/Y	G/H	J/O	K/Q	M/S
"	27	123	BPF	B/V	D/X	F/Z	I/K	J/P	L/R	N/T
"	28	135	CQG	A/G	C/W	E/Y	K/Q	M/S	O/U	
"	29	241	DRH	B/H	D/X	F/Z	J/M	L/R	N/T	P/V
"	30	352	ESI	A/G	C/J	E/Y	M/S	O/U	Q/W	

The sequence continued more or less in this style till February 14. Later (March 20, 1942) stepping on the ringstellung came into force again along with the old stecker pairing. Thus from March 20 to 26 we got the following series of ringstellung, stepping two on each wheel -- AOD, CQF, (ESH), GUJ, IWL, KYN, MBP. (Note that the bracketed ringstellung is an inference and that there is a slight deviation in the last of the series.)

Brown II has a less colourful career. When it was first broken in quantity in January 1942, it obeyed the stecker pairing rule and apparently continued to do so till April 14. Four later April days (26-29) show no stecker rule at all, but late in June the stecker pairing was again observed. Brown II never observed the self-stecker block rule, nor the stepping rules, nor did it ever use only five stecker pairs: it confined itself to the normal Brown practice of six or seven stecker until the fateful day, October 12, 1944 when Brown II was broken and proved to have ten stecker -- like any common or garden key.

This discovery was a great shock, as it suggested that Brown was at last abandoning its peculiarities, now endeared by long association, and coming into line with other keys: and apart from sentiment the use of ten stecker would inevitably make Brown harder to break by ruling out the stecker pairing rule and eliminating the traditional resource of the "clonk" -- see the History

of Brown in a later chapter. Although Brown II quickly disappeared, these forebodings were not unwarranted: for on July 15, 1943 Brown I adopted ten stecker and Brown III, a new key that appeared in the autumn of 1943, had ten stecker from the beginning. Yet despite the loss of its main hallmark the Brown keys always retained a place of their own: to the end they used consecutive stecker freely and refused to adopt any of the normal Air key rules.

1·42 G.A.F. KEY REPEATS

1·420 Institution of Key Records

In the summer of 1941 records were started of the component parts of the keys recovered, i.e. wheelorder, ringstellung and stecker. The records were instituted on the assumption that as discriminants were known to repeat it was possible that the other parts of keys were also likely to be used again. From the account of the discriminant system it can be seen that this was completely wrong but the time spent in compiling the records and in their upkeep declared considerable dividends.

1·421 Limitation of the Subject

For the purpose of this report one class of key repeat is ignored. This is the one where a back key is used again, either as a day-for-day repeat or in some form of shuffle, because of the non-arrival of the current key. The detection of these was a routine matter and presented little or no inconvenience. This was particularly true as in the majority of cases we were forewarned by reading the message giving the German units concerned the necessary instructions. The repeats under discussion are those made deliberately in the construction of keys. It is interesting and ironic that, from the evidence, it seems that repeats occurred in greater numbers whenever, as a security measure, additional keys were introduced. Presumably the extra labour required so infuriated the key compiler that he resorted to repeating portions of old keys.

1·422 Local Keys

Before covering the larger field of keys constructed by the Cipher Office it may be interesting to look at locally-made keys. Where the status of a unit did not officially entitle it to a key of its own, but circumstances arose which made one necessary, then the unit applied to its Luftgau for one. Such a key was made up by the Luftgau without reference to the Cipher Office. Whether this was regarded by some of the Luftgau as an imposition is not known, but it was quite common for such "sonder" keys to be constructed from others. Noteworthy were the following examples.

(a) Scorpion II and III. Fliegerführer Afrika, during the campaign of the winter 1942-3 employed, apart from his official key, two others. Scorpion II was a shuffled version of Primrose of the month before and Scorpion III a shuffled Blue of the month before.

(b) Crab (Fliegerführer Luftflotte 1) in August 1942 employed a hatted version of Wasp of June 1942.

(c) Yak (Fliegerführer Kroatien) was a consistent repeater but showed originality in that it used to employ back versions of itself as a basis for keys.

1·423 Keys Constructed by the Cipher Office : Repeats in 1941

Although repeats appeared in these keys throughout the war, "fashions" were continually changing. However, a historical account is the easiest way of discussing the various types of repeats.*

May 1941 Red of the 18th and Violet of the 1st had the same stecker. There was no "diagonal" or other pattern to the stecker so that the repeat can only have been deliberate. However, no other Violet days were broken and the repeat was not discovered until two

* The following account covers the whole period of the war and so exceeds the time limits normally observed in this chapter. Most the repeats, however, arise in the period 1941-3. Some additional remarks on the later repeats will be found in section 1.58

or three months afterwards when the records were being compiled so that no capital could be made of this.

September 1941 Red stecker repeated Red stecker of February 1941 on a straightforward day-for-day basis with the exception that as the basic month had only 28 days, some days were used twice. This meant that once the pattern of the repeat,was established (about the 4th of the month) the rest of the month was broken by hand. This was providential as it coincided with the start of General Auchinleck's offensive and enabled us to concentrate all our bombes on other important keys, such as Light Blue and Chaffinch.

1.4.24. 1942 : Quadrilateral Repeats

This year was the zenith of the repeats. The effects upon the various sections of Hut 6 organisation were far-reaching. January 1st marked the introduction by the Germans of separate Fliegerkorps keys and an increased number of Luftgau keys and this extra labour apparently caused the Cipher Office to adopt the expedient of repeats on a wholesale basis.

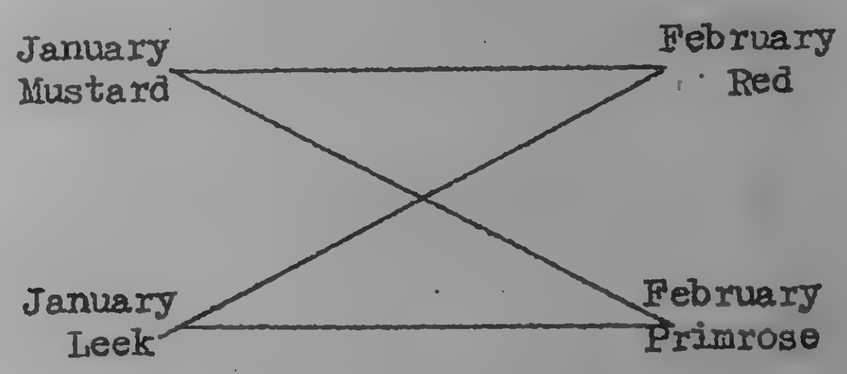
The January repeats gave little indication of what was coming. They were

(a) Hornet stecker repeating Light Blue, July 1941
(b) Leek stecker repeating Blue, July 1941 and
(c) Primrose and Gadfly sharing the same monthly set of stecker.

The three repeats were not on a day-for-day basis but were on patterns which were discovered and this enabled us to determine beforehand which back day's stecker had been used.

February brought the first of the "Quadrilateral Repeats".

The key compiler made a set of keys for one month in the normal manner and then cut them in half: wheelorder and ringstellung in one half and stecker and discriminants in the other. These halves were then united differently and issued as keys for the next month. This practice was symbolised by us as:-



where the diagonal lines represent wheelorder and ringstellung and the horizontal lines represent stecker and discriminants. From the diagram it is obvious why these repeats came to be called Quadrilaterals.

The habit grew steadily from one quadrilateral in February to ten in October and December. When it is realised that ten quadrilaterals meant repeats from twenty keys of November into twenty keys of December it can be seen that the possibilities for breaking are many. Further assistance was given us after the first quadrilaterals in February by the fact that the "Reverse Quadrilaterals" appeared. This system meant that when we found that Mosquito and Leek of July had been used to compile Primrose and Snowdrop of August we could be certain that Primrose and Snowdrop of July

were the basis for Mosquito and Leek of August. The beauty of the system from our point of view was that part of the repeat could be established from the external characteristics of the traffic i.e. a discriminant repeat meant a stecker repeat.

1·425 Effects on Our Breaking Policy

Our breaking policy had to be completely revolutionised. Previous to the quadrilateral repeats, pressure of time had forced us to abandon a key if it was unbroken within a few days. It now became extremely important that as many keys of the first day of the first month of the pair should be broken. This was so that any repeats in the second month of the pair should be established as soon as possible and even as late as September 28th we broke Cockroach of September 1st. Having assembled an assortment of keys for day one of the first month the messages of day one of the second were examined for discriminant repeats from the month before. Any such repeat meant that the stecker also repeated and by combining this stecker with the available wheelorders and ringstellung in turn the resultant keys were tried until a German text was obtained. In this way the repeats were established in a very short time and, as an item of interest, Blue of October 1, 1942 was broken before midnight on September 30th owing to the difference between German time and G.M.T.

1·426 Effects on Our Intercept Policy

Before 1942 the lack of sets and intercept operators had forced us to discourage vigorously the taking of any traffic on a key which could not be broken or which was not operationally important. With the introduction of the quadrilateral system, however, this policy had to be revised. No one could tell whether a very minor but breakable key might not be partially repeated by an operational and vital key in the following month. To meet this contingency the so-called "Insurance Policy" was introduced. By this system daily cover was arranged so that known cribs on all keys were intercepted and then the group dropped. In this way, even if the keys were never attempted during the current month at least the cribs were available in the following month if needed.

The following are extracts from "An Appreciation of the Enigma Situation, June to December 1942" written by Welchman and Colman.

(1)"..... the key repeats which were expected in August could only be exploited by maintaining cover on the minor G.A.F. groups during July and there was no means of knowing which would prove to be useful..... A good deal of bombe time was used in August on the minor G.A.F. keys but some of this was applied to the breaking of July keys which helped to break August keys with a resulting decrease in bombe time spent on Red and the principal Mediterranean Air keys in August. In all 396 G.A.F. keys were broken in August for 5719 bombe hours, an average of 14 bombe hours per key, against 138 keys in July for 7549 bombe hours, an average of 55 hours per key. Thus the key repeats not only increased the number of breaks but also reduced the total bombe time and enabled more bombe time to be spent on the Mediterranean Army keys."

(2) "The history of Locust deserves special mention. One day was broken in January and one in March. As a result of the scanty knowledge of the traffic obtained from these two breaks it was possible to break Locust again in June, at the time of a Malta convoy, with the help of a cilli and a partial key repeat from May Foxglove. Nineteen days of June Locust were then broken but breaking could not be continued in July. In August a key repeat led to

the breaking of nearly all the July days as well as nearly all the August days. In September breaking again stopped although crib cover was fully maintained, and in October a key repeat again made it possible to mop up most of the previous month's keys as well as most of the October ones. In November when the key became of first-rate importance operationally (the North African landings) the knowledge gained enabled us to go on breaking without the assistance of key repeats although a heavy expenditure of bombe time was needed.

(3) "..... it was possible to discover cribs in some of the minor air keys and to arrange special crib cover during September. One result of the October repeats which has since proved to be important was that Celery was broken for the first time and was found to possess a good crib."

Such was the record of 1942 but the next extract from the appreciation sounded a note which unfortunately proved to be true.

(4) "..... it appears that the man who prepares the G.A.F. keys is changing his habits and that the repeats may not be quite so helpful in the future as in the past.

1·427 Repeats in 1943 and 1944

The repeats continued in 1943 but on a very much reduced scale and in a more complicated and less helpful manner. Four keys of one month were separated into their four component parts, shuffled and remade into four keys for the next month. This meant that discriminants no longer gave any assistance and repeats could only be established after an initial break had been made and then only if the corresponding day of the basic keys had been broken in the previous month. This lengthened the odds against our discovering the repeats.

Between April and July 1943 there was prevalent a habit of issuing exactly the same key on four key sheets but with different discriminants. This was completely unexpected and was naturally only discovered when two of the four keys involved were broken and compared. After the practice was discovered then every time a key was broken a mammoth all against all decoding had to take place until it was established which other sets of discriminants decoded on the key. This had to be done every month as the sets of four keys differed monthly.

In the last three months of 1943 the only repeats found were confined to the ringstellung. The monthly set of ringstellung for a key of one month was divided arbitrarily into three or four blocks of days, the blocks shuffled, and used for another key for the next month. The number of blocks made from a monthly set and the days comprising the blocks varied from key to key. This coupled with the fact that from our point of view the ringstellung was the least difficult part of the key to find made the repeats of little value to us.

During 1944 repeats were almost non-existent so far as we could establish. However, towards the end of the year one or two isolated cases of stecker repeats did occurr.

1·428 Stecker/D Repeats in 1945

The introduction of Reflector D pairings as an integral part of a key led to repeats being found of a completely new character. In the past repeats always occurred between parts of a key serving the same function but in 1945 cases were found where stecker pairings had been used to construct reflector pairings.

The original records for finding repeats were known as "Parkerismus" and were kept up by hand and the necessary comparisons made by eye. D pairings employed 24 letters (excluding J and Y) and stecker only 20 and the manual system of recording, instituted in 1941 did not permit of comparisons between the two

On the principle that with the G.A.F. Cipher Office "you never knew" it was obviously worth making the comparisons and therefore a new and mechanical method was devised of recording and comparing stecker and D pairings. These comparisons showed three cases of five common pairings and one of four but the outstanding results were the following:-

A	Snowdrop	A	D	E	F	G	H	I	J	K	W													
	22.1.45.	U	Q	S	Z	M	N	O	V	X	Y					B	C	L	P	R	T			
	Red D	A	D	E	F	G	H	I		K			B		P			C	L					
	1st Period	U	Q	S	Z	M	N	O		X			W		V			R	T					
	1/45																							
B	Snowdrop	C	D	H	I	L	O	P	Q	R	U													
	18.1.45.	J	Z	M	S	N	V	T	Y	W	X		A	B	E	F	G	K						
	Hyena D		D	H	I	L	O	P		R	U	C								A	B	E		
	1st Period		Z	M	S	N	V	T		W	X	Q								F	G	K		
	1/45																							

The partial repeats can be dismissed as happening by chance but the two given in detail are obviously the result of deliberate intention. This is further proved by the pattern of the changing process.

When considering this process two points should be borne in mind:-

(1) when constructing a D plugging J and Y, by the construction of the machine, must be omitted.

(2) for some unaccountable reason the G.A.F. Cipher Office had a deep-rooted objection to pairing consecutive letters together, either in a stecker or in a D.

The process seemed to be this:-

(a) lift all pairsnot involving J and Y directly into the D

(b) the letters to which J and Y are paired in the stecker are paired together in the D. If these letters are consecutive (as in example A) the process is altered - see (d) below.

(c) Take the unsteckered letters in alphabetical order and pair them 1 and 4: 2 and 5: 3 and 6: These obviously cannot give consecutive letters.

(d) Where operation (b) gives a consecutive pairing take the offending letters and pair them with the 1st and 4th unsteckered letters. The remaining unsteckered letters are paired 2 and 5: 3 and 6 as in (c) above.

The pattern of the dates of the stecker used can also be explained. The monthly key list of the G.A.F. Cipher Office is dealt with fully in the section on G.A.F. Discriminants and in January the 1st read

Red
Indigo
Gorilla
Beetle
Hyena
Jaguar
Gadfly etc. etc.

INFO
REC

From this it can be seen that January 22nd fitted to Red gives January 18th up against Hyena. It is therefore obvious that D pairings have been allotted to the keys in their Cipher Office order and that stecker pairings have been used in consecutive day order to provide those D pairings.

This has all been gone into in great detail because it was never able to be proved further owing to the fact that although every key issued had D pairings printed on it they were not all used. Thus we did not obtain the necessary evidence to corroborate the theory, but the theory is sound and had D been more widely used it is extremely probable that we should have been able to reconstruct the pairings, at least for January 1945, without having to break them.

1.429 Conclusion

It must be emphasised that, theoretically, if the enemy is not breaking your keys then you can use repeats, partial or otherwise, as much as you like, although there is a chance that a capture may give you away. If, however, you feel you must use repeats then use them in a completely patternless manner so that even if the enemy does establish that one key is constructed from another he can only ascertain which day is used for which day by breaking both without the aid of the repeat.

From all this it seems that one of the most desirable attributes of a key compiler is full confidence in the ability of the opposing cryptographers.

INFO
REC

1·43 GENERAL ORGANISATION OF MACHINE AND CRIB ROOMS, LATER WATCH AND RESEARCH

1·430 The Fourfold Division

During this period there were four separate sub-sections directly concerned with breaking: M.R.1, M.R. Research (or M.R.2), C.R.1, C.R. Research (or C.R.2). M.R.1 and C.R.1* dealt with operational colours on a current, three-shift basis: M.R.2 and C.R.2 dealt with all other colours on a non-current basis, i.e. examining the traffic on an average two days late, with the ultimate object of handing over to the routine shifts any colour that could be worked up to a point where it was currently breakable, provided, of course, that its intelligence importance justified the transfer. M.R.2 and C.R.2 worked in general on day shift.

This fourfold division grew up by degrees. M.R.1 was the lineal descendant of the Machine Room of the early days of Hut 6; C.R.1 was formally started in October 1940 (though cribs were first used in August): M.R.2 first began in autumn 1940 but it was not for the best part of a year that it had any permanent or assured status in the shape of a fixed nucleus of members. The early routine of all these sections has already been described. C.R.2 came much later: it began on a very small scale in April 1942 but cannot be said to have got going as a permanent organisation till September 1942 when D.M. Gaunt took over its organisation.

1·431 Location of Rooms

M.R.1 and C.R.1 were necessarily always located in neighbouring rooms at the nerve centre of Hut 6, centrally placed for communication with Registration Room, Decoding Room and the bombe huts. One of the party, normally a member of C.R.1, was in direct control of the bombe situation. M.R.2 and C.R.2 were by no means so fortunate and lived a very nomadic existence: Hut 6 was simply not large enough for its inhabitants and so sections not strictly necessary for operational breaking had to seek accommodation outside. After several migrations M.R.2, C.R.2 and the corresponding Registration Room, R.R.2, found rooms in the Main Building which were satisfactory in themselves but inconveniently remote from the rest of the Hut, a matter particularly awkward in 1942 when the vagaries of key repeats caused frequent tie-ups between research and current colours. Finally the space problem was solved by the completion of Block D and the transfer of all sections of Hut 6 to premises which seemed at the timo palatial, an illusion speedily dispelled.

1·432 Subordination of Sub-sections

Administratively both sections of the M.R. were under one head (Major D.W. Babbage) as were both sections of the C.R. (Mr. P.S. Milner-Barry). Now this administrative division cut clean across the division of keys with which the various parties dealt: for M.R.1 and C.R.1 dealt with operational keys, M.R.2 and C.R.2 with non-operational. But there were graver objections than purely technical administrative anomalies to the illogical system that had grown up. As was eventually realised by all the leading figures of the Hut, the M.R./C.R. division was wrong in practice.

* M.R.1 and C.R.1 as the operational sections of M.R. and C.R. were frequently referred to without the numeral: but here for the sake of clarity M.R. will be used to refer to M.R.1 and M.R.2 together and so with C.R. M.R.1 and C.R.1 were also referred to sometimes as the routine shifts.

1.433 The Differentiation of Function

In terms of work the distinction was as under. The M.R.'s responsibilities included keeping an eye on Rules of Keys, cillying and keeping cilli records, organising hand attempts, making up bombe menus, dealing with the bombe stations on technical matters, testing (or supervising the testing of) bombe stops and finally seeing to the prompt completion of the correct story. The C.R.'s responsibilities were keeping crib records up to date, discovering cribs and handing them to the M.R. to be made up, finding and working on re-encodements, controlling what was being run on the bombes and keeping in such close touch with the W/T background as was necessary for the efficient discharge of the above duties. Certain functions, such as working on depths or rodding, fell within the uncertain borderline between the two Rooms.

Now it is obvious that there is something very artificial and arbitrary in this division of responsibility between the two sides of breaking and indeed Hut 6 could never have got on without the closest liaison between M.R.1 and C.R.1. Every day questions would arise which neither party could settle on its own. Was a crib produced by the C.R. strong enough to run on wheelorders contradicted by a rule or a cilli ? Again it might happen that the M.R. would discover one or two cillies, but not enough to run i.e. to make up into a bombe menu: then they had to approach the C.R., cillies in hand, and ask if cribbery could supply a beginner or signature for the message concerned. Similar questions would arise between M.R.2 and C.R.2, and at one time a system was adopted by which the M.R. after examining blists noted any cillies and wheelorder preferences in a special notebook which was later consulted by the C.R. But all such makeshifts emphasised the illogical nature of the barrier that had grown up, and moreover, there was always the danger of some important scrap of information not being passed on.

1.434 Dissatisfaction in the Machine Room

The M.R./C.R. divorce had another consequence which should be mentioned as an illustration of the evils that may arise from an error in organisation. During the summer of 1940 the M.R. had been the nerve centre of the Hut: but as cribs became the main standby this altered and by the autumn of 1941 the boot was very much on the other foot. C.R.1 was in the ascendant and its members alone were in close touch with the intelligence authorities in Hut 3 and were alone in a position to make vitally important decisions of bombe policy. Meanwhile the members of M.R.1 (with only occasional hand breaks to console them) felt themselves degraded from their former proud position to be little more than menu-makers and testers of stories - not that these occupations are in themselves useless or dishonourable but they were too routine and mechanical to occupy the full powers of the persons concerned. Hence there was considerable dissatisfaction in M.R.1*. This feeling came to a head in the autumn of 1941 when several meetings were held to try to find a solution: in 1942 while the grievance remained the situation was not so acute as new M.R. methods of breaking, in particular the dottery, provided a temporary palliative.

* M.R.2 for reasons to be mentioned later had not so much of a grievance. Still it must be remembered that at this time most members of M.R.2 were temporary visitors from M.R.1 so M.R.2 could not fail to be to some extent influenced by the general M.R. discontent.

While one does not wish to exaggerate the discontent engendered and while anything like an actual explosion was avoided it would be false to deny that this was a serious crisis in personnel management. Fortunately, however, the problem was successfully solved. Once the faulty system was corrected the staff difficulties vanished, proving thus that they were caused not by personal incompatibilities but by organic maladjustments.

1.435 The Problem Solved

So in 1941-2 we were faced with two evils: (1) there was an artificial distinction between two aspects of breaking and (2) the machine experts were being relegated to a position that did not give sufficient scope to their abilities. Clearly the proper solution to both difficulties was to unify the two sides of breaking: and all parties agreed on this as a desirable reform. But reforms, however desirable, cannot always be carried through at once; and to attempt an immediate amalgamation would have led to chaos as neither party was ready to take over the other's work. Technical knowledge had first to be interchanged. So a series of visits was arranged by which members of M.R.1 spent a week or two in C.R.1 and learned the routine, and vice versa: and finally, when it was considered that this preparatory fusion had gone far enough, the formal amalgamation was arranged. For reasons of practical convenience its execution was deferred till shortly after the move from the old and cramped Hut 6 to the spaciousness of Block D; and in February 1943 M.R.1 and C.R.1 married as the Watch, set forth on a new and auspicious career. At the same time the Netz Room (now a valued auxiliary to the other cryptographic sections) assumed the time-honoured title of the Machine Room.

1.436 The Formation of Research

At the same time a similar amalgamation took place between M.R.2 and C.R.2 who united to form the Research Section. The Watch was placed under the control of Mr. Milner-Barry, formerly head of the C.R.; and Research under Major D.W. Babbage, formerly head of the M.R. This removed the administrative anomaly mentioned earlier.

This amalgamation also had been prepared beforehand by tuition in M.R. methods given to the members of C.R.2 and by cribbery on certain keys carried out by M.R.2. However, in the Research sections the division between M.R. and C.R. had never been so rigid, and so the fusion presented a simpler problem. The reasons for this difference are interesting.

Because (at least in 1940) the natural means of entry into new keys was by cillies, the M.R. speciality, M.R.2 was as we have seen inaugurated much earlier than C.R.2. However, in the early days breaks secured by M.R.2 were examined by C.R.1 from the crib standpoint. But it soon happened that C.R.1 whose numbers were for some time far too small for their growing responsibilities, became so occupied with cribbery and re-encodement work on important operational colours that little time was left for sustained effort on the less urgent research cribbery: and at the same time some members of M.R.2, realising the artificiality of the distinction between M.R. and C.R. methods, began on their favourite and adopted keys.* to make independent investigations into the field of cribbery. So, when the staff

* I.e. The keys of which they were the parents (see later).

INFO
REC

situation at last permitted us to establish C.R.2 as a separate sub-section, there were already certain keys which by long-standing agreement were treated for cillies and cribs alike by M.R.2, and this arrangement - which suited both parties, as C.R.2 had its hands full with other work - was allowed to continue till the formation of the unified Research Section. The keys that were thus wholly taken over by M.R.2 were Brown (when it was not a routine commitment), Orange I and II, Mustard and Quince. In addition, when the eventual amalgamation was definitely planned, a number of other colours, such as Cockroach and Snowdrop, were taken over for periods of varying length by M.R.2 members. So in fact long before the fusion, M.R.2 and C.R.2 had done much to break down the wall of partition, and had already secured unity of control on certain keys.

1.437 The Parentage System

This seems a suitable moment to discuss the parentage system, an essential part of the organisation of Watch and Research. This was a system of specialisation virtually forced on us by the rapid proliferation of keys. In Hut 6 history about 200 distinct Enigma keys were identified, named and broken and sometimes nearly half of that number existed simultaneously. No one person could have anything but a general knowledge of this vast key complex. In 1940 and even 1941 one man might still cover the whole field in some detail; but later this was impossible. What could still be attained was a thorough knowledge of machine technique, a mastery of the theory of cribs and re-encodements, a general knowledge of a large group of keys - usually Air or Army which it became clear were separate key systems - and a detailed and intimate acquaintance with several keys within this group. Hence there grew up - more or less simultaneously in the C.R. and M.R.2, though the word, I think, is a C.R. invention - the parentage system, by which one (or sometimes more than one) person "adopted" - i.e. made himself responsible for the welfare of - a certain key or group of keys. (This was, of course done with the approval of the head of the section concerned, and did not affect his ultimate responsibility for breaking.) The parentage system, however, though already existing in embryo, did not come fully into force till the Watch/Research set-up was achieved, as only from then on did parentage imply full responsibility for both cribs and cillies.

The dangers inherent in an excess of specialisation were seen and guarded against. Changes in the allocation of keys to parents were made at intervals, sometimes at short intervals; and hence many members of Hut 6 had parental experience of a number of different keys. These changes were supervised by the head of the section or sub-section concerned: his general objects were to dispose of his cryptographic resources to the best advantage i.e. to make full use of the special talents of each individual, to ensure that each key got its fair share of attention (in the light both of intelligence value and cryptographic possibilities), to combat the enemies of boredom and staleness by shifting round the duller and more hopeless tasks and, finally, to see that everyone had enough to do but not more than he could reasonably be expected to cope with. (This last was sometimes difficult when the work of the section was either very busy or very slack but, if necessary, transfers of staff to or from other sections were arranged). Apart from this general post at intervals, it was expected that every member while specialising in his own colour should take an intelligent interest in the remaining work of the section.

It should also be mentioned that parenthood had a somewhat different meaning to Watch and Research - a difference that arose inevitably from their varied methods of work. Research parenthood (on keys that were broken with any frequency)* was a full-time occupation: normally the parent did all the work on his key, examining blists, preparing menus to be run on the bombe and entering the traffic when the day was broken. (Normally Research keys were decoded in bulk, then sent to the parent for examination before being passed on to Hut 3). This ensured the individual supervision of records that is especially valuable on difficult colours; and in general Research keys were more difficult than Watch ones. In most cases there was also no urgency in breaking; hence on a parent's day off his work could simply be left over, though naturally a foster-parent had to take over during long leave.

By contrast Watch parenthood was part-time, and though the parent is spoken of in the singular, all major Watch keys had more than one parent. The parent's main duty was to look after the general interests of his child, and in particular to keep crib records in a systematic form. In the Watch the breaking of keys of operational value (as most were) had to be a continuous process; therefore every member might have to take a hand in breaking any Watch colour, and so had to know something of all Watch colours. Any member might discover and prepare cribs to be run (though the decision as to what should be run was reserved to the head of shift) and in general the entering of Watch traffic was performed e.g. by a person on each shift set aside for this sole purpose - not necessarily the parent of the key being entered. Thus it was never the case that on Watch keys the parent did all the work: the burden was in fact one that varied very much with the state of the key and the enthusiasm of the parent. It was also generally true that the busiest time for a Watch parent was when his child was sick for then he had to nurse it back to health; and the busiest time for a Research parent was when his child was in vigorous health, for then he had a lot of entering to do.

From 1942 on there was an intermediate category of colours looked after by the Q-Watch or Qwatch^{Ø}, a body of cryptographers who worked (mostly on Air keys) in the closest collaboration with the Watch proper - in fact in its early days the Qwatch was often called the "fourth Watch" to distinguish it from the three routine shifts. The Qwatch looked after keys which for some reason - e.g. difficulty or inferior intelligence value - were not suitable for full Watch treatment but were yet so closely connected with Watch colours that it was judged inexpedient to banish them to the outer darkness of Research, and also on occasion nursed back to health full Watch keys that had "gone bad". There was normally indeed a lively interchange of both keys and personnel between Watch and Qwatch. Qwatch methods were essentially a compromise between those of Watch and Research: its members worked on more current material than the researchers, but specialised rather more than did the Watch proper, and did most of their entering by bulk. In the last period of the war the Qwatch idea gained ground markedly and eventually as we shall see ousted the older Research conception.

* [illegible] broken parenthood was more honorary. [illegible] at any [illegible] out method of seeing that no key [illegible] plete [illegible]

[illegible] division of the Wate

INFO
REC

1·438 Some Special Points

The reader may feel inclined to ask two questions - (1) Why is it that Hut 6 made in 1940 what was later recognised to be a radically unsound distinction between M.R. and C.R. ? and (2) How was it that this unsound division and the tension it caused made so little difference to the practical success of Hut 6 ?

The fundamental answer to (1) is probably that the art of Enigma cryptography found its main development in a different direction from what seemed likely in the summer of 1940: then it looked as if cillies (helped by Rules of Keys) were to be the trump card, and the majority of cryptographers were so fully occupied with pursuing this line of attack that they neglected the alternative of cribs - not then usable in the absence of the bombe. It is possible that had the bombe been with us a few months earlier the cilli method would not have got such a start over the crib method and so not have attracted such an excessive preponderance of attention and effort. Ultimately the error was a natural enough failure to forecast correctly future developments: one moral is that we should never neglect to develop a new breaking technique even if at the time it seems unlikely that it will be required. (Compare the technique of the dottery, worked out in 1941 at a time when it seemed unlikely that we would have many occasions for using the method, which came into its own in 1942 as a consequence of an unpredictable series of key repeats.)

The answer to (2) is partly that the evils were counteracted by close liaison between the parties concerned. But the fundamental answer is that the practical success of a section such as Hut 6 (so far, at least, as the directly cryptographic work is concerned) does not depend primarily on a faultless internal organisation - desirable as this may be to secure smooth working in all departments, Granted that the nature of the cipher is known and that a practical method of breaking has been devised, success will be measured by (1) the provision of staff adequate in numbers and quality and (2) the provision of sufficient mechanical aids - i.e. in our case, sufficient bombes. Perfect organisation is at best in the third place, and the success of Hut 6 is due to the fact that on the whole throughout the war the above two conditions were well met.

1·439 Summary

The final moral of the M.R./C.R. story may be stated thus. While in a complex cryptographic organisation like Hut 6, a considerable degree of specialisation is unavoidable as between interception, traffic analysis and cryptography, it is undesirable that there should be any watertight divisions in the initial processes of breaking. Any specialisation that is necessary here should arise from divisions of the material to be broken - e.g. Watch/Research and later Air/Army - not from different lines of approach to the same material.

After the fusion all members of Watch and Research looked at the problem of breaking as a whole and used M.R. or C.R. methods as best fitted the occasion. The routine of the Rooms in such matters as a separate log for each key approached more nearly to that of the crib sections, but there was a general unification of records. Research was comparatively soon again divided into Air and Army Research and this was a forerunner of the final reorganisation to be described later.

INFO
REC

Successful as the fusion undoubtedly was, it would be untrue to say that the old M.R./C.R. division left no traces. It had gone too deep for that to be possible and, as has been said earlier in the Introduction, the two aspects of cryptography do tend to appeal to different types of mind. Though many became equally versed in both techniques, in other cases the original bias and native forte was always discernible. But such a degree of specialisation is desirable; granted the general knowledge of the whole breaking process that was secured by the success of the fusion, there was everything to be gained by permitting individuals to pursue the higher levels of theory in accordance with their particular bent. Fortunately also it happened that throughout this history of Hut 6 there was work to be done suited to all varieties of cryptographic taste and talent. So in the final period - January 1944 to the end - when cillies were least important, the use by the Germans of Reflector D and Enigma Uhr presented new technical problems and allowed us to gather a belated autumnal harvest from the gnarled tree of machine theory.

On the general questions of the rival merits of the cilli or crib method of breaking honours must be adjudged even. If for the greater period of Hut 6 most breaks were secured on cribs, the initial entry into many important keys was made on cillies and without cilli breaks we would not have obtained our invaluable crib evidence. The value of cilli breaks is thus immeasurably greater than any mere calculation of their number can show. If we wish to sum the merits of the two lines of approach in a sentence, we can say that M.R. methods first broke the Enigma and C.R. methods kept open the breach: but to say which was more important is to ask whether it is the upper or lower blade of the scissors that cuts the paper.

INFO
REC

1·44 TRAINING SCHEMES IN HUT 6

1·440 Early Training

The need for special courses of training for new members of Hut 6 was first felt in the autumn of 1942. Before that time, training had been essentially individual. New members of the Hut would be given an introductory talk on the machine and a series of subsequent talks varying from section to section, but no effort was made to build up training schools or to draw up programmes of work in progressive courses. Training came from doing the work itself, in the company of others who had been doing the work for long enough to gain experience of the routine and knowledge of the techniques. A member of the Machine Room,* for instance, would have to learn not only about the machine in general, but also about the exploitation of cillies, the making of menus, the working of the bombe and a mass of other technicalities, for which members were considered good learners in view of their particular interests and previous education. In the Crib Room the entering of typed books provided the quickest means of learning to recognise and discover cribs. The visiting system in the C.R. and M.R. gave a chance for this individual system of cryptographic training to be put to good use. It was considered useful psychologically to introduce members of the Registration Room and Netz Room to the broader aspects of the work of the Hut. They came as visitors, and saw something of the final process in the handling of Enigma traffic. Promising pupils who showed a special aptitude for key-breaking might be retained in the Watch or Research. Other pupils, it was believed, would go back to their routines refreshed and invigorated, and see the final purpose of their often tedious work. Throughout the general maxim was applied that experience is the best teacher.

1·441 The Beginning of the Schools

It was with boom conditions of work and with a steady increase of staff from the end of the University year 1941 - 2 that the need for more formal and planned instruction arose. The members of the Decoding Room required a good deal of practice and some instruction, and this section led the way. In August 1942 it was decided to set up a D.R. School, and after difficulties of space had been overcome, it was duly inaugurated on September 14th. The Registration Room School followed later in the same month. Here new staff were taught the background of blisting - a little about W/T, the system of key distribution and naming and the various registration routines - and given supplementary talks by other members of the Hut on such topics as discriminants, methods of breaking and Control. Visits to the Bombe Hut and to Sixta were also arranged to catch a glimpse of the wider picture and see the wheels go round. The course was useful enough to be extended in scope. In October it was used as a refresher course for members of the R.R., who had not previously had the opportunity for any systematic tuition.

* This section covers a period during which the term "Machine Room" was used in two senses. To avoid ambiguity in the present section Machine Room is used in its original sense referring to the machine cryptographers, and the older term, Netz Room, is used for Machine Room in its second sense.

In the pioneer organisation of the R.R. School were laid the foundations of the systematic training of all new members of the Hut and of the specialised cryptographic training for members of Watch and Research. If 1942 saw a great increase in the totals of D.R., M.R. and R.R. staff, 1943 saw the largest single increase from outside to our cryptographic staff that had ever taken place. No new member from outside the Hut entered the cryptographic sections between January 1942 and April 1943. Then the flood-gates were opened. First three members arrived from Bedford, then a batch of four undergraduates from Cambridge in the early summer, then a bunch of Americans. There was also a further intake of cryptographers from the M.R., the R.R. and the D.R.

But it was not merely a question of increasing numbers. The scope of the work was becoming more difficult at this time. The fusion of the M.R. and C.R. meant that the knowledge of the average member had to be more varied than ever before, and, in the case of the new member, a great deal more had to be learned at once. Most of the new arrivals were not mathematicians, and the machine side of the work demanded systematic and detailed instruction. However, it was not until the arrival of the University intake that a Watch Course was drawn up. The earlier arrivals in 1943 did the R.R. School Course and followed this up with a week in the Qwatch, entering typed books and having an occasional talk on bombes and cillies. Three weeks' probationary work was then done in the Watch; this consisted of one turn on each of the shifts, while the prospective member learned the routines by helping to carry them out. Sometimes one or two weeks followed in Research, particularly for individuals whose success was not quite certain.

In June 1943 a committee was set up to see how this system, which had been applied in the case of visitors, could be improved and extended to cater for the University intake, and a detailed plan was drawn up. It was agreed that all new members of the Hut destined for the Watch should go first to the R.R. School, where they would learn something not only of other people's problems, but also of the cryptographic background as a whole.

1·442 The R.R. School Syllabus

At this point the R.R. School, with a course which lasted for a fortnight on a two-shift basis, became a much more formal institute of instruction than before. It is worth while appending the Syllabus, first drawn up in October 1942.

(I) W/T

(1) Wireless Sending, Morse etc.;
(2) The Organisation of a Wireless Station: Signals Office, Operators etc.;
(3) The Message itself: Preamble (Frequency, Length, Callsigns and How to Look them up, Discriminants, Practice in Colouring the Register etc.): Text (Five-figure Groups, Dupes etc);
(4) Wireless Working: Use of Callsigns, Control and CQ, Stars, Kreis, Netz etc.

(II) The Machine

(1) Details of Turnover Mechanism, Ringstellung Clips, Tyres, Stecker etc.;
(2) Keys: Setting up a Key;
(3) Encoding and Decoding Messages: The Indicator System;

INFO
REC

(4) Cillies and Ringstellung Tips: How they Arise

(III) Hut 6 Routines

(1) Blisting: Practice;
(2) Naming of Keys: Traffic Summaries;
(3) Routine Jobs in R.R. 1 and R.R. 2: Control Jobs;
(4) Key Repeats;
(5) Fag Systems

(IV) Elements of Breaking: Bombes, Menus etc.

This ambitious syllabus was taught by varied methods. The Course as a whole was in the hands of an experienced member of the R.R. (in one case of the N.R.), who was competent to deal with certain aspects of the Course very well. The bulk of the Course, however, was taught indirectly by means of papers, which had been drawn up by experts in their respective fields. Much was also put across in lectures by "outside" speakers, including members of the Watch and Research. Visits were arranged wherever possible, and the whole of the syllabus was designed to be as practical as possible, and to give unity and direction to the work of the Hut as a whole.

1·443 Watch and Research Training

For those members going on to Watch or Research a further Course was now drawn up, systematising a good deal that had never been systematised before. The syllabus was drawn up in two parts: (I) The Machine; (II) Cribs and Re-encodements. The first part of the Course was expressly designed to give a much wider machine background to members of the Watch than was general at the time.

Part I

(1) Cillies: Their Nature and Types: Practice in Subtraction of Cillies and Deducing Wheelorders: Breaking on Cillies;
(2) Ringstellung Tips: How to Find them;
(3) Hand Attempts: Difference between English and German Ringstellung: Females: The Cyclometer etc.;
(4) Breaking on the Bombe: Cribs and Menus: What the Bombe does: Its Construction: Different Types of Bombes: Jumbos: Different Types of Menus: Cilli Menus: Hoppities;
(5) Rodding: Theory and Practice

Part II

(1) General Talk on Cribs: Statement of the Problem: Routine Messages: Spotting the Crib Message: Guessing what it Says: Aids in Spotting the Message - Length, G.T.O., Callsigns etc.;
(2) The Crib Folder and Conventions of Entering;
(3) Types of Cribs and Different Forms of Cribs: Cycles: Security Methods against Cribs - Location of Address, Wahlworts etc.;
(4) The Preparation of a Crib - Unduped and Contradicted Letters, Checking of Unduped Teleprint etc.;
(5) Talk on Re-encodements: How they Arise: How they are Spotted: Fitting the German: Stagger Stretches: Teil-Breaking: Linked Stagger Stretches: Routine R.E.'s: Comparison Cards and Folders: Partial R.E.'s: R.E.'s from Non-Enigma;

V V
INFO
REC

(6) Talk on the Organisation of Watch and Research;
(7) Stray Points to be cleared up:
(i) Boils and Form Sheets,
(ii) Depth,
(iii) Construction of Keys,
(iv) Rules of Keys
(v) Sources of Information,
(vi) Crib Cover

The main method of driving these points home was by means of twelve practical exercises, based where possible on "real life" examples and graded in terms of their difficulty.

1.	Hand Attempt:	Cillies plus Ringstellung (Keyboards)	Rating: Easy
2.	Hand Attempt:	Cillies plus Ringstellung (Nearnesses)	Easy
3.	Depth Reading:	Robinson Fun and Games	Moderately easy
4.	Re-encodement Exercise		Difficult
5.	Depth Reading		Easy
6.	Hand Attempt:	Cillies plus Ringstellung (Various)	Difficult
7.	Dottery		Easy
8.	Dottery		Moderately easy
9.	Dottery		Moderate
10.	Dottery		Difficult
11.	Re-encodement (Panzer R.E.)		Moderate
12.	Hand Attempt		Moderate

In the second part of the Course and in the supervision of the exercises various members of the Watch acted as instructors and guides. Parents were detailed to talk about their own keys and the Qwatch became a School, attached to the main establishment. Various improvements were suggested in the arrangement of the Course. With a large number of keys, the week or more of entering in the Qwatch had become somewhat dull and monotonous, and the last groups of people to do the Course had this week extended and interspersed with days of routine shift, working on the keys on which they had been instructed. After this experience of current working, they went back to the Qwatch for a spell of two or three days' revision. In the case of the American contingent , a special room was set aside and the Course was given in a class-room atmosphere with competitive impetus, at least in the solution of the exercises.

By these means, new members of Watch and Research were given a wide background before setting out as fully-fledged operational staff. In the Watch itself, there was still something to learn of the division of labour and the allocation of jobs, and it became customary to send all new members to work for at least a week in the N.R., where they would not only test stops and find ring-stellung, but learn something of the liaison with the Bombe Hut and its outstations. The N.R. itself had a vast amount of educational training to carry out, for its numbers increased more rapidly than those of the Watch, and it was losing experienced members regularly to Watch and Research. Special papers were written outlining the work of the Room and members were gradually initiated into the more specialised tasks.

1·444 The Outline Course and Special Talks

The value of the Watch Course as a general introduction to Enigma and its breaking was plain, and it was felt that an outline course on the same lines would be of value to others besides the

members and potential members of the Watch. So a Short Course was drawn up to last two or three days, which could be attempted by visitors from other departments. It was divided into three lessons, each of which lasted preferably for a day.

Lesson 1: The Machine and Hand Breaking
Lesson 2: Bombe Breaking by Cribs and the Finding of Ringstellung
Lesson 3: Cribs and Re-encodements and How to Find them

Each of these lessons had its appropriate exercises.

For members of the R.R. in training, talks on the work of the Watch were regularly given by members, who would discuss not so much the different methods of breaking as the part played by Watch and Research in the total effort of Hut 6 as a whole. The ideal method of tackling a key would be considered as a problem - and the value of complete traffic, tidy blists, comfortable hours and expert attention being balanced against urgency and speed in the breaking of operational keys. The Watch would become a demonstration centre for interested and curious novices, who would have the functions of the different shift members explained to them on the spot.

1.445 Other Educational Schemes

Three other detailed educational schemes need some attention in this discussion of Hut 6 methods of training. The first was the special Menu-making Course inaugurated in December 1943 and developed in 1944, when members of the R.R. were drawn into the cryptographic organisation to relieve pressure, particularly on the Army Watch. They were taught in two main lessons.

Lesson 1: Machine Turnover: Cribs: Why Written out in Banks of 26: The Turnover Assumptions implicit in Menus and the Meaning of the "Relative Positions of Constatations": Types of Stretches chosen for Menus: Strength of Menus: Practical Menu-making: Methods of Menu-making - Ringing "Females" and Noting Triangles, Checking, Phantoms and Bracketed Letters, Bombe Copies etc.

Lesson 2: Top and Tail Menus: Cilli Menus: Hoppities: Delayed Hoppities

These two lessons were supplemented by much practice work, and, of course, it was merely necessary to be taught the essentials of this subject in order to set off on the job. Practice was the best teacher.

The second educational scheme was organised in collaboration with Sixta, and was designed for training T.I.S. members. After the abolition of the regular use of discriminants in September 1943, it was felt that T.I.S. members should be taught something of log reading, D/F and other branches of W/T. A Course was arranged and held at the end of 1943, but, because of pressure of work, it was never possible to give everyone the opportunity of taking the Course.

The third educational scheme was connected with the Hand Duenna attack projected in July 1944 to meet the dreaded extension of Reflector D. When it was found that there was no immediate need to put into effect the complicated organisation prepared beforehand, the enterprise was transformed into a trial run. It

INFO
REC

was unique in so far as it demanded a detailed educational training for Wrens at Stanmore as well as members of the Hut itself. Four bays of bombes at Stanmore were to be put out of action, releasing sixty Wrens per shift. These Wrens were to be taught and supervised by one shift leader from the Hut. The understanding of the Hand Duenna technique required a Netz Room background, and those with this knowledge and experience were well supplied, under the leadership of the Technical Adviser (O.H. Lawn, a member of the Watch), to do the teaching of the shift members. Many members regretted that the scheme had not to be undertaken operationally, but the teams at Stanmore did a trial run, which would have been of considerable value in facing new contingencies.

This was the last general experiment in training. From this time until the end of the war, new technical problems and new situations were faced by existing staff and techniques evolved by a progressive adaptation of existing knowledge.

INFO
REC

CHAPTER 1·5

PERIOD V : JANUARY 1944 - MAY 1945 : THE LIBERATION OF EUROPE : HUT 6 FIGHTS BACK AGAINST NEW GERMAN SECURITY DEVICES

INFO
RECD

1·50 GENERAL HISTORICAL SUMMARY

1·500 The Determining Factors

Complicated in the extreme as is the detailed history of Hut 6 in the final phase of the war, the main determining factors can be briefly stated. They are two in number:-

(1) The decisive assault on the Fortress of Europe launched on D Day.

(2) The bringing into force of new German security measures.*

It will be convenient to discuss the effect of these factors under four main heads, viz. the technique of cryptography, the organisation of the cryptographic sections, the importance of other sections to cryptography and the contribution of Hut 6 to intelligence.

1·501 The Technique of Cryptography

The new devices introduced by the Germans (in particular D and Enigma Uhr) brought about a remarkable renaissance of machine theory. Old problems that had in the past seemed merely academic - and also new problems - had to be tackled and mastered. The space assigned to D and Uhr in the technical volume is a fair measure of the scope and extent of the theoretical developments. In particular, the invention and improvement of D-breaking machines was (so far as Hut 6 was concerned) the climax of cryptographic mechanisation.

1·502 The Organisation of Cryptography

This was scarcely affected by the new German devices, but underwent many changes both in anticipation of D Day and as a result of it. The main developments were the transference of the principal Western Air keys to the Watch in May 1944, the setting up of the Army Watch just after D Day, and (as a consequence of the general contraction of the fronts and the increased interlinking of previously separate keys) the gradual alteration of our whole breaking set-up from a Watch/Research to an Air/Army basis. This important development - the last major administrative change in Hut 6 - was finally completed at the beginning of December 1944 and is fully discussed later.

1·503 Importance of Other Sections to Cryptography

A marked feature of the whole period is the increased dependence of the cryptographer (wandering in the confused labyrinth of W/T camouflage - culminating in callsign encoding - and the key compromises inevitable in fluid warfare) upon the helpful thread of the traffic analyst. Inevitably liaison with T.I.S. and Sixta became ever closer. T.I.S., in particular, took over two important cryptographic functions: (a) responsibility for the identification and naming of "unknown" keys - in particular, the Barnyards; (b) responsibility for dealing

* In so far as these are strictly cryptographic, they will be fully discussed in the following sections.

with captured keys* i.e. identifying the keys and seeing that any available traffic was decoded.

1.504 Contribution of Hut 6 to Intelligence

The new German security measures of all kinds might, properly handled, have virtually stopped the flow of operational intelligence from Hut 6 to Hut 3; very largely through German mistakes, this result was never achieved. However, this is not to say that our success was unaffected: several keys (in particular Puma) were finally ruined by D, and the encoding of callsigns on the G.A.F. caused a serious drop in Air decodes from which we never made a complete recovery. But on the whole the luck of Hut 6 held good, and to the end we decoded currently most of the vital operational traffic.

From the standpoint of the quantity and quality of the intelligence sent to Hut 3, 1944 was our peak year. The peak period - for quantity at least - is probably just about a fortnight after D Day when for about a week in the keybook over 30 keys appear as broken on each day. The statistics of the total number of breaks put 1944 easily above other years: in 1942 through the incidence of key repeats it would sometimes happen that more keys would be broken at one time but there are many months in 1944 that top the 1942 record of 550 breaks.

On the Army side, in particular, 1944 witnessed an immense advance. Though we should not forget the valuable intelligence provided by the African Army keys in 1942-3, still Hut 3 had never previously seen Army traffic of such high quality as on the best keys of 1944 - the Bantams, Ducks and Puffins. The importance of Army keys relative to Air constantly increased and towards the end when the Air difficulties were most acute the Army decodes sometimes surpassed the Air in number as well as quality. This was, of course, a reversal of the situation that prevailed for most of the war: but the Army experts who had had in general the hardest cryptographic tasks cannot be grudged this final hour of triumph. In 1944-5 first Italy, then the West, finally even the East was held in fee and on the Army as on the Air the cryptographic encirclement of Germany was complete.

To sum up, on the standards of quantity of breaks, quality of intelligence and general all-round cryptographic success 1944 saw Hut 6 at its best: at the height of its resources in personnel and machine power the Hut worked flat out, particularly in the weeks immediately following D Day. By the unanimous testimony of the generals in the field, the contribution to victory now made through the ULTRA intelligence which flowed to the Continent as regularly as PLUTO'S oil can scarcely be overrated: though it must be remembered that the success of 1944 could never have been achieved without the patient spade work of the preceding years, it is none the less true that on the final analysis, 1944 was Hut 6's finest hour.

* In the last year of the war Hut 6 was constantly under fire from an increasing barrage of captured documents and machines. The documents after examination by T.I.S. were filed and catalogued by the Chief Cryptographer, Major D.W. Babbage.

INFO
REC

1.51 GERMAN SECURITY DEVICES AND OUR COUNTER-MEASURES: REFLECTOR D

1.510 General Introduction

Between January 1944 and May 1945 the Germans introduced a large number of security measures. Some were of a W/T camouflage nature and are thus dealt with in other sections of this report: they had, of course, their effect on cryptography in so far as they made proper traffic identification more difficult. Other enemy measures, however, were essentially cryptographic i.e. they affected the actual process of encoding and thus influenced our methods of breaking.

It will be convenient to classify the various devices adopted into three groups and then consider them in turn. The groups are (a) mechanical gadgets which involved the provision of an addition (or Zusatzgerät) to the standard Enigma machine; (b) alteration of the key; (c) encoding rules, and the separate devices adopted are as under:-

(a) 1. Reflector D
2. Enigma Uhr

(b) 3. Zusatz Stecker
4. Notschlüssel

(c) 5. CY
6. Random Indicators
7. Wahlworts
8. Mosse Code
9. Double Encoding

Before proceeding to discuss these devices in turn and the counter-measures we adopted one or two general points should be noticed. Firstly, these new German tricks were of very unequal value and importance: as might have been expected, technically D and Uhr were far more important than the rest, and indeed D as a potential menace to our cryptographic success was much more serious than the rest of the bag of tricks put together. Class (b) was a minor nuisance to the cryptographers but not much more: while class (c) did not on the scale used fundamentally affect our breaking methods though they did make breaking more expensive and difficult.

Secondly, it should be stated that while the German security drive of 1944 was on a more thorough scale than previously, some of the devices had been used earlier or were on the lines of measures previously adopted. Such pre-1944 anticipations of the 1944 devices will be referred to later under individual cases.

1.511 Reflector D in General

Uncle D, as he was familiarly known, was a household word in Hut 6 from January 1944 to the end: for the first half of the year he was also shrouded in a black cloak of mystery and the secret of his true identity and nature gave rise to much ingenious speculation. In what follows it is proposed to discuss Uncle D and all his works in historical sequence, making clear at each point the extent of our knowledge: in the technical volume the reader will find a full discussion of the methods used for breaking reflectors.

INFO
REC

D, as it affected Hut 6, was primarily a G.A.F. security device; and this at once leads to a division of the history into two sections:- (1) January to July 1944; (2) August 1944 to May 1945. Up to and including July 1944 D was confined to Red among G.A.F. keys: from August on its range was extended and consequently the number of D's recovered rose rapidly. From January to July we recovered 21 D's: from August to the end of the war 379.*

1.512 January - July 1944

The First Menace On December 23, 1943, Hut 6 received an unwelcome jolt. A Red message was intercepted on a Norwegian frequency which gave instructions that a new reflector - called Umkehrwalze Dora - was to come into force on January 1, 1944. It was not clear from the message whether the new reflector was to be used on part of the Red system, or on all of it: or even whether it was to be confined to Red at all. We felt there was a reasonable chance that the Germans would make the error of using the new reflector only on a part of Red; but we had to make preparations for the less favourable possibility that Red as a whole might go over to the new reflector and thus at a stroke become unbreakable by our normal method - the bombe.

Hut 6 was then suddenly faced on little more than a week's notice with the possibility of a first-class cryptographic crisis which was liable to result in the loss for an indefinite time of the principal G.A.F. key, Red, the cornerstone of all Air cryptography and still at the top of the intelligence ladder. Recurrent crises were not unusual in Hut 6 at this time: only recently in November 1943 the Germans had dropped the regular use of discriminants on the Air and a radical change of W/T set-up was now expected every month. But this was a crisis of a new order: a new reflector, if it came into universal use, would (until broken) make all our hundreds of bombes so much waste metal. Till we had solved the D mystery our whole breaking technique was jeopardised.

Yet while no one minimised the gravity of the impending crisis and the seriousness of the ordeal through which Hut 6 might have to pass, it would be wrong to imply that the cryptographers viewed the prospect as an unalloyed tragedy. It had been so long since they had been forced to direct their minds to the higher reaches of theory that many felt a distinct exhilaration at the thrill of a difficult problem. The very completeness of our conquest of the Enigma, the very perfection of our technique seemed at times to make it all too easy and monotonous. Certainly 1944 was destined to dispel quickly any such feeling: D was only the first (though the most serious) of a host of new problems. Yet probably most of those closely involved in the solution of these new difficulties would agree that the increasing interest of the work was on balance a more than adequate compensation for the additional labours involved.

Meanwhile preparations were made in the last week of the year 1943 for the worst i.e. that Red would go over wholly to D. At the time there was only one way to tackle the problem - i.e. to break by the hand S.K.C. method+ on a long crib (which could

* This later figure includes just over 100 by capture

+ D-breaking machines were not yet in existence nor thought of.

probably only be attained by a R.E. from some other key). It was realised that if D was universally introduced our only chance was a R.E. from some other cipher: but there was nothing we could do about this but wait until the 1st and see what happened. We could, however, - and did - hold a number of meetings at which the technique of S.K.O. was explained and discussed. In all this activity Mr. Alexander, Head of Hut 8, was prominent and his experience - for Hut 8 had had to use S.K.O. on several occasions - was invaluable.θ These meetings were attended by the cryptographers of Watch and Research plus selected personnel from the M.R. From this band it was proposed to draft a team for the S.K.O. operation if necessary while those not selected would have to go on breaking in the normal way any keys unaffected by D.

It must be remembered that at this stage no one had or could have any conception of the true nature of D. It was thought of as a fixed reflector like B or C: we were prepared for a hard struggle to break it but it was imagined that once broken our troubles were over. Herein ignorance was bliss: the stoutest hearts might have quailed in those last days of 1943 had it been possible for us to realise the hydraheaded nature of our veiled antagonist.

Illusory Triumph Perhaps no single day in Hut 6 history was more memorable in prospect than our D Day, New Year's Day 1944. Breaks that on other days had become matters of course recaptured their old thrill and any who had forgotten in daily routine the meaning of our achievement had a fresh realisation of the truth of the statement "The breaking of Enigma is a daily miracle".

The first break was that of Leek at 1100 hailed as never was a Leek break before or since as it proved that D was not a universal presence. This was followed by the vital break of Red at 1150. All the traffic already in came out on the key we had discovered and for some time we wondered whether Uncle D was but a false scare. But after dinner it became clear that messages on the Norwegian Auto and some on the G.H.Q. Auto were not coming out. A reasonable beginner SEQSXFREDX was then rodded on one of the Norwegian messages, assuming the Red stecker, wheelorder and ringstellung (which gave the turnover on the rods). What was obviously the correct story was discovered, but there was no hole through the Jeffreys sheets: therefore the presence of a new reflector was proved. The rodding was then continued through the middle wheel and the wiring of the reflector established by Oliver Lawn at 0130 on the morning of the 2nd.* D was unmasked and the crisis was over - or so we fondly thought. Alas for the vanity of human wishes! How soon was the cup to be dashed from our lips!

The BO Mystery For the moment, however, the skies were clear. Arrangements were made to have bombes, hand machines, and D.R. machines fitted with the new reflector: this could easily be done by plugging and in fact within the first week of January at least one Red key was broken on a crib run on D. Meanwhile a set of D

θ While the technique was known in outline, few members of Hut 6 had any practical experience in S.K.O. The method had never been successfully employed in Hut 6 - no doubt, of course, because the need for it had never arisen.

* For the process employed see the technical volume. The method soon became routine and was eventually speeded up by new apparatus: but this was the first occasion we had required to use it (except for the break of reflector C on cillies in 1940).

rod catalogues was ordered to be a companion to the existing B set and the hypothesis that Greenshank was on D and hence (as we supposed) now breakable was canvassed. But on January 11th Uncle D struck again.

The D traffic did not come out on the wiring already known. In the same manner as before a new wiring was recovered which had one pairing and one alone - BO - common with the first D. This discovery at once showed us that D was a many-sided device and a much more formidable threat than we had imagined. To anticipate events, we found that approximately every 10 days a new D came into force on Red and every D had the common pairing BO. Up to the end of July, 20 Red D's were broken and given serial numbers.

A great controversy followed as to the nature of the device. Argument turned principally on the significance to be attached to the fixed pairing BO but it was by no means clear what theory this peculiarity supported. Two main theories were propounded - (a) that D was pluggable and hence each of the countless possible variants would have to be broken individually when used or (b) that D was a device with a limited number of positions and hence capable eventually of a complete once-for-all solution. Various ingenious theories on the nature of this device were suggested by the imaginative members of the Hut: the simplest idea was that D consisted of a basic fixed reflector with another thin wheel next to it rotating through 26 positions. This was in accordance with naval practice: and if it had been true we could have broken the basic D on three positions (assuming D 1, 2, 3, were in point of fact consecutive) or on some seven or eight, if the succession of D's was random. The main weakness of this theory is that it is at least unlikely that a common pairing would have appeared in such a D-family.

It is, however, needless to pursue our speculations in detail. Largely from the difficulty of forming any other watertight hypothesis, the pluggable theory steadily gained ground, and was finally proved correct by the capture of the Red key-sheet for June 1944 with the D pairings on it. To remove all doubt, the column containing these pairings was headed STECKERVERBINDUNGEN AN DEN UMKEHRWALZE. The D pairings were written vertically in three columns of four pairings each: for the month there were three D's, each covering approximately ten days.

The D Substitution The reader will notice that we have spoken of twelve pairings only. Now our D's had thirteen pairings - twelve variable and the fixed pairing BO. It was therefore clear from this discrepancy alone that the German system of notation for D pairings was different from ours but as we had previously broken some of the D's now captured it was easy to work out the relationship between the two systems. The transformation is shown in the following table:-

ENGLISH	GERMAN	GERMAN	ENGLISH
A	A	A	A
C	Z	B	Z
D	X	C	Y
E	W	D	X
F	V	E	W
G	U	F	V
H	T	G	U
I	S	H	T
J	R	I	S

ENGLISH	GERMAN	GERMAN	ENGLISH
K	Q	K	R
L	P	L	Q
M	O	M	P
N	M	N	N
P	L	O	M
Q	K	P	L
R	I	Q	K
S	H	R	J
T	G	S	I
U	F	T	H
V	E	U	G
W	D	V	F
X	C	W	E
Y	B	X	D
Z		Z	C

It will be noticed that (starting from A = A) one alphabet runs backwards and the other forward omitting the letters BO in the English alphabet and JY in the German (which correspond to the permanently fixed pairing).

The discovery was important in two ways:- (1) for its reference to Rules of Keys and (2) because in the future we could translate captured D's into our own notation. Naturally, however, for all general purposes we continued to use the English notation.

Greenshank and D So far we have spoken of Red D's only and it is true that so far as the G.A.F. was concerned D was so far confined to Red. But even before the end of 1943 there was a strong suspicion - based on the failure of several good Falcon R.E.'s - that Greenshank, the prize of prizes for Army Research, was using a new reflector or a new wheel. The gradual growth of this suspicion is clearly seen in the reports of the period as confidence of success is replaced by baffled dismay: and so strong had the suspicion grown that the best R.E. - on October 7, 1943 - was run through all Naval wheelorders and reflector combinations at Washington.

It is therefore not surprising that Army Research quickly decided that D was the answer to the Greenshank riddle and strong psychological stories that appeared early in 1944 were run unsuccessfully on the then known varieties of D. Success however, obviously depended on the truth of the "limited variety" theory of D and as the pluggable theory gained ground the running of Greenshank on known D's was more and more discouraged.

The possibility remained of a break by S.K.O. and in any case there was a strong feeling that whether we broke a Greenshank day or not a S.K.O. experiment was well worth undertaking for the sake of practice: we might yet have to do the job in dire earnest. Accordingly towards the end of February 1944 a team of four people with occasional visitors conducted an experimental attack on Greenshank of October 7, 1943. This failed to break the day (probably because it was not possible to press the attack home - only two out of five right-hand wheels were tried) but (as the report made properly emphasises) gave useful information on the best technique to adopt. The time that would have been required to do the complete job was estimated at about a fortnight for relays of five people working continuous shifts.

It is emphasised, however, in the report on this experiment that the best method to tackle any particular S.K.O. problem can only be determined in the light of the peculiarities of the available crib. In a favourable case the time required may be much reduced. This point was quickly driven home by one of the great personal triumphs of Hut 6 - the break of Greenshank of April 27, 1944 on a re-encodement of some 200 letters. This feat was effected in about a week by taking full advantage of an equidistance in the crib and gambling on our chances, by trying only the most favourable hypotheses to reduce the labour involved to proportions that a lone worker could contemplate. It was universally recognised as a fitting reward that Fortune should have at length smiled upon Lionel Clarke, who had chased Greenshank with relentless determination for four long years.

This break made it highly probable that Greenshank was using D as the BO pairing appeared,* and this suppostion was fully confirmed by the later Greenshank breaks in 1945. We were soon able to establish that the companion key (for, as is elsewhere explained, Greenshank used two keys on the same day) used the same D: but we could break no days near at hand by running on the D we had recovered. But though the truth was early suspected it was not until much later that we were able to demonstrate that Greenshank changed its D daily.

Red D's: January to July Meanwhile the Red D's were being broken regularly and with no great difficulty. It was soon discovered that there was some uncertainty about the date when the second and third D's of the month would come into force: but this caused little serious trouble in practice. During these relatively quiet months the members of the Air Watch got constant practice in breaking D's and a general speeding up of the process was soon achieved by the construction of suitable tables and the convenient invention of the "half-enigma". The only breaks in the steady progressions of three Red D's a month were caused by two Red compromises. Curiously enough in the first case (March) the reserve key came into force on the 10th but no D was used; hence in March there is only one D. But in June the reserve key (which came into force in the middle of the month) had its own D, and so we got four D 's in that month. The conclusion is obviously that in March the reserve Red key had no D's printed on it while in June it had.

The Overhanging Menace But during all this period we could never forget the sword of Damocles. Of course we were more or less all right if things went on as they were: but we could not rely on the Germans always making the egregious mistake of using B and D on the same key. It was clear that sooner or later there would be a great extension of the use of D: the references in decodes to the continuous distribution of D's to units were decisive on this point. Sooner or later, it was clear, D would extend to more keys: and some fine day we might discover that Red or possibly some other even more important key would be unbreakable as being "wholly D" or "nearly wholly D".

So all through this period while the T.I.S. experts classified all references to D, noted its distribution and endeavoured to discover the principles underlying its use, the Uncle D committee, under Mr. Alexander's chairmanship, held regular meetings to dis-

* The D was named DG 1. At a much later period it was given a D number in the regular series, and was then called D 194.

cover if possible a real defence to the menace of a "wholly D key". Most attention was paid to mechanical D-breaking devices; for it was realised that though we might have in an emergency to use hand methods they were too slow and too expensive in the labour required to be really feasible as a means of operational breaking. Machine experiments were set on foot, both here and in America; and as a result the various D-breaking machines described in the technical volume were evolved. Of them all, Duenna - a machine invented by American experts as a result of discussions with Mr. Alexander who visited the States in connection with this problem - proved in practice most successful:+ and a hand method, known as Hand Duenna, was elaborated as a stand-by in case the full crisis came on us before the machines were ready.

Had the Germans known how easily they could have checkmated us! Yet to imagine this presupposes that they had some idea of our successes against the Enigma and it is clear they had no conception of the extent of our victory. Also, slow as their proceedings seemed to us, it may be that they were in fact distributing D's as fast as they could. In any case the first day of every month (in spite of several alarms) passed with no change in the situation: but at last it became apparent from references in July, that something was really going to happen on August 1.

Preparations for August 1 Elaborate preparations were made for August 1 - our second D Day. Careful co-ordination of records was clearly necessary and this was organised by the Qwatch while through the parents of various keys a list of Air cribs was drawn up with special attention to any that offered possibilities for Duenna or hand S.K.C. Except for a few special frequencies which had declared their position in advance, it was impossible to predict what messages would be on B or on D and careful assessment of probabilities would clearly be required before we could give up a key as "wholly D". On the Research keys the class of those that could be broken or failed on B within a few days but were hopeless on D was distressingly large. This was due of course, to the greater demands of D-breaking machines compared with the bombe (see the figures in the technical volume) and boded ill for our prospects if there was a serious extension of D. But with the perennial optimism engendered by so many narrow escapes in the past we still hoped that the Germans would continue to mix up B and D and so in the popular phrase hand us their reflectors on a plate.

1·513 August 1944 - May 1945

Extension of D To a considerable extent our optimism was justified. By August 2 three distinct D's had been broken,[o] Red, Cricket and Gadfly, and others rapidly followed. There was no significant extension in the use of D on Red and at least five keys - Ocelot, Puma, Yak, Snowdrop and Daffodil - were free from D. There was also no appearance of D on Army Keys.

However, it was not long before we realised that the nightmare of a wholly D key was no fantasy. Wasp, the key of Fliegerkorps IX,

+ It is only fair to remember that it had a start over most of its rivals.

o This disproved the pleasing illusion that all keys might share a common D.

went over wholly to D on August 5:* the first and not the least serious of our defeats by our shadowy antagonist. Later the Wasp D's for the second and third periods of August were recovered by running shots on the only non-D frequency - the Nosegay fag: but it was obvious that Wasp as a nearly 100% D key was hanging by a hair.

From later evidence and our general knowledge of the G.A.F. cipher office it is possible to state that what really happened in August 1944 was this. Prior to August 1944 only the Red key sheet had D's printed on it. Now it is believed that in the G.A.F. cipher office a number of keys were made up and then the key number and discriminants added in a fixed order which determined the nature of each key. On this theory not till the discriminants were added was the nature of the key known: thus before August 1944 the Red D must have been made up when the discriminants were added and not when the key was composed. But from August on it is simplest to suppose that every key when made up had its quota of D's added before the keys were identified by number and discriminants. At any rate this theory is not contradicted by the available evidence.

On this theory it follows that from August 1944 every G.A.F. key had a set of D's attached, i.e. every key was liable to use D. But it does not follow that every key did use D: firstly, certain units might not have D distributed to them; and secondly even if an operator had D, there is a lot of evidence to show that D was so unpopular with German cipher clerks that they would not use it without explicit and repeated orders. It is possible from our actual breaks to draw up the following table of the first use of D on various keys:-

August	1944	Gadfly, Cricket, Jaguar, Cockroach, Snowdrop, Hyena, Wasp, Pink, Lion, Mosquito
September	"	Beetle, Gorilla
October	"	Mustard
November	"	Puma, Narcissus, Yak, Daffodil, Leopard
December	"	Ocelot
January	1945	Aster, Lily
February	"	Skunk, Wallflower, Indigo
March	"	Marmoset, Moth
April	"	Gentian

This table gives a general picture of the gradual increase in the extension of D: but it should be borne in mind that (especially in the case of rarely-broken colours) it does not follow that the month in which we first recovered a D is that in which D was first used on the key in question. It is very likely (to cite examples) that Skunk, Marmoset, Indigo and Gentian used D before the dates given above. It is also true that the general tendency towards more use of D was sometimes reversed: for example, Gadfly which used D in August was again all on B from December 1944 onwards. German cipher clerks reverted to use of B whenever the pressure of security officers was relaxed. Thus there was a constant fluctuation in the use of D which over any given period would decrease in some localities and increase in others: the over-all tendency, however, was undoubtedly towards increase.

* This was at the time a deduction from its failure to come out but was proved later.

INFO
REC

Effects on Breaking While at the end of the first week of August we could not but feel that we had escaped more easily than we might, the long-term effects of the extension of D soon became apparent and (from this and other causes) from August till the end of the war there was a steady increase in the difficulty of breaking most G.A.F. keys.

In the first place, the problem of recovering the D even when the rest of the key was known was no longer the formality it had been on Red. Red was a large key with at most times a plethora of reasonable cribs: most other keys were in a less happy state. One might break into one day of a key on B and find no suitable crib on which to recover the D: of course, one solution was to break another day in the same period, but this was not always easy and in any case involved delay. To meet this case various ingenious methods of breaking a D on a known key without a crib were devised and sometimes employed with success*: but again all these methods were fairly laborious and none so certain as breaking on a crib. Again, apart from difficulties caused by lack of cribs complicated technical problems were raised when a key was broken on B and virtually all the remaining traffic was on D and Uhr. Moreover, the difficulties of key identification caused by the general absence of discriminants, callsign encoding, key compromises and in the East the endemic uncertainty of the key distribution added to the effect of the technical snags already described. It was often impossible to know whether a message dud on one key was on that key plus D or on another key used in the same neighbourhood. Now no cryptographer worth his salt is dismayed by a tricky technical job if he is reasonably sure of his ground: but it is to say the least a daunting prospect to embark on a laborious attempt to break a D when the odds may be against the message you are working on being on the assumed key. Thanks to the cumulative effect of all these considerations, it would sometimes happen that a D would not be broken despite B breaks in the period even when a D was believed or known to have been used.

In the second place, special problems were provided by "nearly D" or "wholly D" keys. A "nearly D" key may be defined as one on which the bulk of the traffic and all or most of the best cribs are habitually on D. It was necessary on these keys to secure an entry on a B crib - not an easy task as they were by definition inferior or fewer - or on a stray B R.E. Exploitation of a break was often easy enough as on good D cribs the D could be found and more days in the period broken quickly: but the initial break was the real problem and because of the time required to effect the first entry exploitation was often far from current. It is thus not uncommon on these keys to find breaks clustering: after a blank period seven or eight Wasps would come out in a few days due to a fortunate initial break. Typical examples of "nearly D" keys were Wasp, Lion, Hyena and Ocelot: the last began using D in December 1944 and, as from then to the end of the war it remained a key of the first importance, there was a constant series of alarms and excursions at the possibility that at any moment Ocelot might become "wholly D". Each break of a new Ocelot D was heralded as a major triumph: but thanks to the errors of the King's enemies we just held on till the third period of April.

* The first occasion was in September 1944 when a Gorilla D was broken by "Bobbery" (see the technical volume).

INFI-
REC

"Nearly D" keys were, of course, in constant danger of crossing the line and becoming "wholly D". Once this fatal line had been crossed nothing could be done except by hand S.K.C. or by a D-breaking machine and in general the labour could not be spared for hand attempts. Greenshank was already known as a "wholly D" key and was joined by Puma on November 20, 1944* and at least one Eastern Front Air key, Skunk, was "wholly D" in February 1945. What we were most of all afraid of was that a vital operational Western Air key would become "wholly D"; but (except perhaps for Wasp at some periods) we were spared this dreaded blow.

D-Breaks The progress of the D-breaking machines under construction in this country and America was thus watched with keen interest and no sooner were the machines in working order than their services were called for on operational jobs. We were in fact compelled by sheer necessity to use highly complicated machinery which was still really in an experimental stage and in all the circumstances the total of eighteen breaks[θ] achieved by the monstrous triad Giant, Duenna and Autoscritcher[+] - is highly creditable to all concerned.

A full list of the D's broken in this way will be found in an Appendix; here it must suffice to mention some of the highlights of the story. Giant - an ingenious makeshift - was the hero of the early days and D 120, Puma of the 3rd period of November was the first mechanically broken D. Considering that Giant demanded a crib of 200 letters, his total of four D breaks is a remarkable achievement. The Autoscritcher was not ready till the last few months but in a short working life showed its mettle by four quick D breaks.

Duenna was the steadiest and most successful machine: she began working operationally in December, was joined in a few months by a sister machine and further reinforced by a third sister towards the end. The Duennas jointly effected ten breaks mostly on Puma.

The breaks of these machines were nearly all on Puma, Greenshank and Skunk - all of which were wholly D as was proved by the decodes of broken days. As we had so few D-breaking machines it was necessary to use them to the utmost advantage: so the principle was adopted of confining them to "wholly D" keys where D-breaks offered the only chance. "Nearly D" keys which gave even a slight prospect of bombe breaks were tried on the bombe. Also as a precaution any job to be sent to a D-breaker was first run on a bombe.

* Orders were issued on Puma to start the use of D on that day: and as it ceased coming out the inference was obvious

θ The figure 18 is the number of D's broken. The number of days that came out in consequence of these successes is, of course, much higher.

+ The war ended before the fourth monster, Ogre, could be used operationally.

In December and January Puma and Greenshank were the competitors for Duenna's favours.* Puma was the easier to exploit if broken and if reasonably current was preferred by the intelligence authorities: Greenshank as relatively virgin soil was the cryptographer's choice. On balance, however, Puma which gave a better chance of success was usually rated higher. The net result was that seven Puma and five Greenshank[9] D's were broken by mechanical means.

It was known that several Eastern Air keys were largely or wholly on D but at first the prior claims of Greenshank and Puma made it difficult to give them their chance. However, Giant's second triumph was the Mosquito D of the first period of February and in the last months of the war Skunk got a good innings and four D's were broken. There is no doubt, however, that the break of the Jaguar D for the first period of April is the most spectacular use made of our D-breaking machines. It was the one achievement which had immediate high operational value.

What happened was that on April 1st Ocelot was broken early and a R.E. to Jaguar D wrote through three teile without alteration. All available machinery was massed in an unprecedented concentration for the attack: at midnight on the 2nd both Duennas and the Autoscritcher were starting up, Giant menus were being prepared and a hand attempt here was already in progress. In less than 24-hours - by tea time on the 3rd - Duenna produced the answer (D 280) shortly before it would have been reached by the hand attempt. This was far and away our most successful attempt at the operational use of D-breakers: but the possible snags were shown by a similar attempt on the second Jaguar D when our whole machinery was tied up fruitlessly for days on end. The trouble was that when the D-breakers failed they took so long to put the job down - which is just another way of saying we had too few machines.

D-Captures In the closing months of the war the military situation led to the capture of many key sheets with their accompanying D's. A large number of these were D's we should never have broken on our own - e.g. the Marmoset D's of March, and a whole series of Indigo D's in February and March. Most sensational discovery of all was the capture of a series of daily changing D's on a slip of paper separate from the key-sheet: the keys involved were soon identified as March and May Grouse (an offshoot of Greenshank). This capture plus the strong evidence of our breaks+ was accepted as final proof that Greenshank changed its D daily.

D Rules The Rules of D, as part of the general subject of

* Giant demanded a much longer crib: so any really long R.E.'s were sent to Giant. CY made it impossible to get a long enough R.E. stretch to run Greenshank on Giant.

9 In addition another Greenshank D was broken by S.K.O., Major Babbage repeating Lionel Clarke's achievement.

+ e.g. The D's in use on March 6th and 7th were different.

Rules of Keys, are dealt with elsewhere: but here we should perhaps mention that the dates when new D's came into force showed considerable variation. From November on every key had four D's a month as opposed to the earlier three: in September and October the practice varies strangely from key to key.

1·514 Summary of the German Use of D

The general question of German cipher security is to be discussed at the end of the cryptographic section of the report: but in the special case of their use of D their cardinal error sticks out a mile. It was a capital blunder to have "mixed keys" using both B and D: any individual key should have been wholly D or not have used it at all. It is the more surprising that the Germans made this error as the Army - which must have used D on Greenshank in 1943 - used the device correctly. The G.A.F. cipher authorities adopted and misused the excellent invention of the Army. D should have been considered an integral part of the key, not an extra.

It may be, of course, that in January 1944 the Germans had not enough D's available to cover all the Red system. But in that event they should have adopted one of two courses - either to introduce D on a part of Red but at the same time to equip these stations with a separate key, or to wait patiently till at one blow Red could be made an all-D key. The effect of a sudden wholesale introduction of D on to selected keys would have been a much more crushing blow to Hut 6 than the slow and piecemeal changes that the Germans preferred. In warfare a new weapon should be first employed in massive strength, not in penny numbers.

Even with all the warning the Germans gave us by their snail-like progress the case of Puma shows what damage a wholly D key could inflict on us. Puma adopted the use of D on November 20th, as it said it would, and subsequent breaks showed it was 100% D - later indeed 100% plus Uhr. From the beginning of August to November 19 our success percentage was 96: from November 20 to the end of February it was 35. (The fall in success would be even more striking if we included March and April when no Puma was broken). Now it is possible that not all this decline is due to D: Uhr played its part and the crib situation also became less favourable. Still the D situation was certainly the main cause.

The reader is invited to answer the question:- If after months of warning (needlessly given to us) of the D menace so that we had the chance of getting D-breakers to work - if even then the Germans by a universal use of D on a key which we had been breaking steadily for months and which we were prepared to run with top priority on our D-breakers could cut down our success ratio by 60% what could they not have achieved by an unheralded universal use of D on a chosen key ?*

* This is, as a matter of fact, what happened on Greenshank. We have good reason to believe that D was in use on Greenshank in 1943 and in view of the German tendency to make important changes on January 1st, January 1, 1943 seems a plausible date for its introduction. If this is so, D was in use on Greenshank for months before we even suspected anything odd and it is at least doubtful whether the Greenshank mystery would ever have been solved had not the G.A.F. done so much to give the game away.

1·515 Appendices

Appendix I D Statistics, Key by Key

Key	Total Number of D's Recovered
Red	57
Jaguar	38
Hyena	27
Cockroach	20
Mosquito	20
Gadfly	13
Wasp	12
Lion	9
Cricket	7
Beetle	13
Gorilla	7
Leopard	16
Puma	7
Ocelot	19
Wallflower	13
Indigo	16
Mustard	5
Pink	5
Aster	5
Skunk	4
Marmoset	3
Moth	3
Narcissus	3
Snowdrop	2
Daffodil	2
Lily	1
Yak	1
Gentian	1
Air Total	330
Greenshank	7
Grouse	62
D for NOT-keys	1
Grand Total	400

In this table the order of Air keys is determined firstly by their order of adopting D (so far as we know) and secondly by the number of D's we recovered.

Appendix 2 Chronological List of D's Broken without a Prior Break on Reflector B

D No.	Key and Date	Broken by	Date of Break
194	Greenshank, April 27, 1944	L.E. Clarke	May 30, 1944
120	Puma, Nov. 3rd period	Giant	Nov. 28, "
150	Puma, Dec. 3rd period	Duenna	Dec. 26, "
160	Mosquito, Dec. 4th period	Giant	Jan. 2, 1945
163	Puma, Dec. 4th period	Duenna	Jan. 3, "
165	Puma, Jan. 1st period	Giant	" 5, "
185	Greenshank, Jan. 14	Major D.W. Babbage	" 24, "
193	Greenshank, Jan. 5	Duenna	" 30, "
196	Puma, Jan. 4th period	Duenna	Feb. 1, "
226	Puma, Feb. 3rd period	Duenna	" 28, "
228	Skunk, Feb 3rd period	Giant	Mar. 1, "
236	Skunk, Feb. 4th period	Autoscritcher	" 6, "
238	Greenshank, Jan. 17	Autoscritcher	" 7, "
241	Greenshank, Jan. 7	Autoscritcher	" 9, "
250	Greenshank, Mar. 6	Duenna	" 11, "
253	Puma, Feb. 4th period	Duenna	" 13, "
266	Greenshank, Mar. 7	Autoscritcher	" 25, "
280	Jaguar IIA, Apr. 1st period	Duenna	Apr. 3, "
326	Skunk, Apr. 3rd period	Duenna	" 30, "
333	Skunk, Apr. 4th period	Duenna	May 6, "

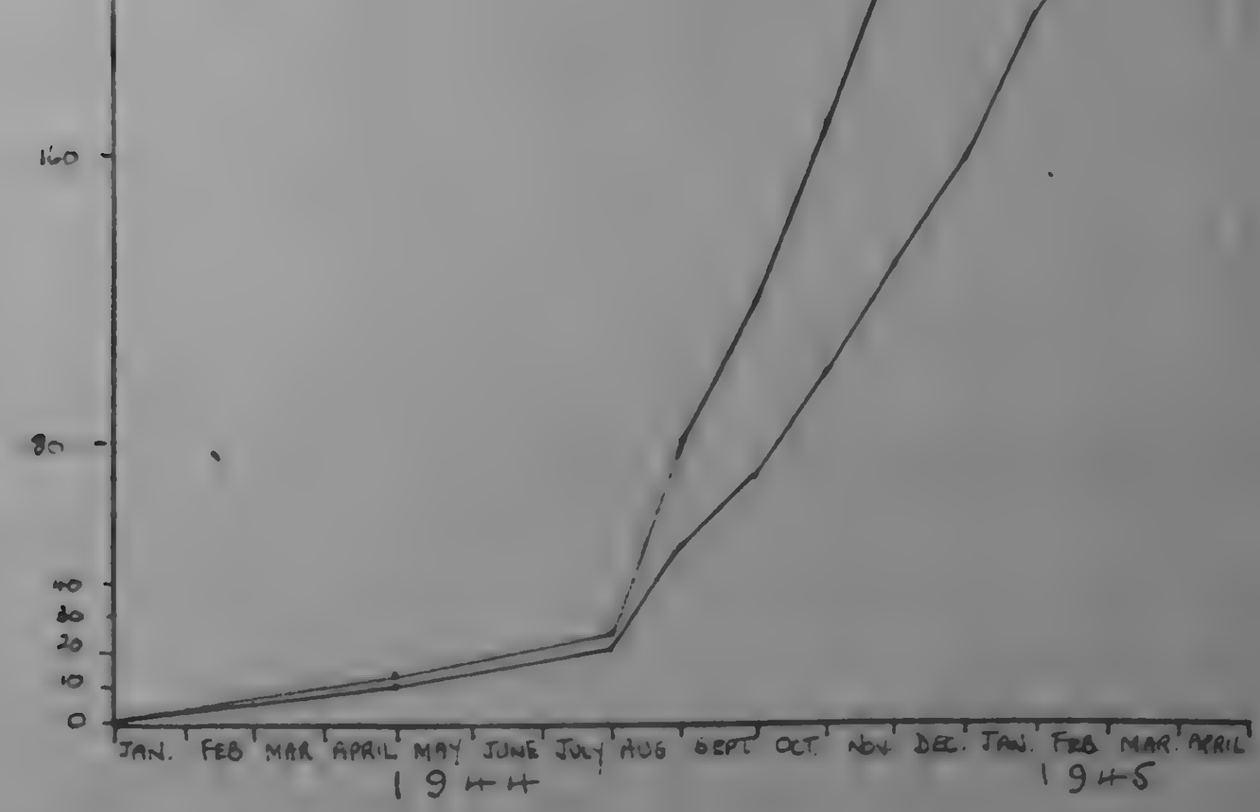
Breaks Classified by Method and by Key

Hand S.K.O.	2	Puma	7
Giant	4	Greenshank	7
Duenna	10	Skunk	4
Autoscritcher	4	Mosquito	1
		Jaguar	1
Total of Breaks	20		20

INFC
RECC

GRAPH of PROGRESS in KELVERING D's

Notes:- —— Estimated number of D's in use.
—— Number of D's recovered.
----- Daily D's per Army (by capture).
The estimated number of D's in use does not include D's used by the Army. Any recovered however, are included in the number of D's recovered, but they are too few to alter the graph materially. All figures are counted to the nearest 10.



INFC
RECC

1.52 GERMAN SECURITY DEVICES : ENIGMA UHR

1·520 The Problem

What is most remarkable about Enigma Uhr is that the enemy succeeded for once in springing a complete surprise on us. The first we knew of it was that on July 10th Jaguar certain messages began with a number[X] and then went off into nonsense. Also a decode referred to one of these messages as enciphered with "Enigma Uhr". It was clear that the nonsense represented an additional re-encoding of some kind on top of the normal Enigma, almost certainly performed by a mechanical gadget.

The first step in solving this problem was clearly to break into one of the Uhr messages and this would have been by no means easy to effect had not the Fusion Room been able to produce a R.E. between a "plain Enigma" message and an Uhr message. By processes that are explained in the technical volume, this R.E. lead to the breaking of the first Uhr substitution - a reciprocal stecker different from the basic stecker. How in the next 48 hours substitution after substitution was recovered (some reciprocal, some non-reciprocal) how the relationship between the various substitutions was worked out and codified and how eventually a mechanical gadget was devised to attach to the Decoding Room machines and perform automatically the variations on the basic stecker - all this will be found elsewhere. To the participants in the rugger scrum in the Qwatch when the complete mathematical theory was being elaborated the whole episode will remain as one of the most tense in the history of Hut 6.

1·521 Routine Adopted

A simple routine was at once adopted[θ] by which the D.R. on discovering the messages marked them "P"(later "H"). The D.R. for convenience in breaking the Uhr decoded the rest of the message and then passed the messages back to the R.R. who entered them upon a special "Plist". A small party in the Qwatch was detailed for breaking the substitutions and passing on the solution to the D.R.

1·522 Extension of Enigma Uhr

Uhr was always an Air gadget and never used by an Army key. Originally used by Jaguar and Cricket only, it was later extended to fifteen Air keys in all[Ø]. It is worth noticing that Jaguar, which soon after the first introduction was encoding nearly half its messages with Uhr, remained throughout the chief Uhr key: the Jaguar Uhr breaks surpass all others put together. For a period in August Jaguar, Snowdrop and Cricket appear regularly in the book of Uhr breaks: then in September Jaguar is the sole survivor and in October even Jaguar deserts Uhr. But in November the use of Uhr starts anew on Jaguar and spreads to other keys. In 1945 the highlights of Uhr's extending kingdom were its first appearance on an Eastern Front key (Beetle) and its appearance with D on Puma and Aster.

X It was soon seen that the numbers ran from 1 to 39.
θ Some inessential modifications were made later.
Ø See Appendix on Uhr statistics.

INFC
REC

1·523 Effect on Breaking

Uhr alone had on the whole little influence on our breaking of keys though it did mean that there was sometimes a lot of technical work to be done after the basic key was broken*. Serious complications arose only when it was necessary to break a key on an Uhr message or when Uhr was combined with D. In running on the bombe Uhr created no serious difficulties in principle - for it was possible by using closures only to allow for the probable non-reciprocity of the stecker - but longer cribs were required and this meant that a colour which used Uhr very extensively and had rather short cribs was made more difficult to break. It is probable that this was in point of fact one of the reasons why we failed to exploit our last two breaks of Fuma reflectors. But if long cribs or R.E.'s were available Uhr was not a major cryptographic obstacle.

1·524 Uhr notation

As has been said above the Germans originally indicated the Uhr number by encoding it with the basic key at the beginning of the message. But in November a method of encoding the number was introduced by which the number was represented by four letters encoded in the basic key at the start of the message according to a simple bigram code (for which see the technical book).

The manner in which this new notation was discovered is interesting. On Jaguar of November there were some inexplicable duds especially on the Abdulla fag. It was thought that these might be on a separate key but several cribs failed. Fortunately someone had the bright idea that the messages might be on Jaguar Uhr with a new method of indicating the number and a message was tried on all 40 sets of stecker. It came out on 28 and showed up the four dummy letters and then the rest was easy.

It will be seen that but for an inspired guess we might not have discovered this new notation for several days. Once discovered, on balance the change helped us: for though it made the recovering of the basic key from an initial Uhr break more difficult it simplified running on an Uhr message as the message had to begin in the fifth place.

A captured document on Enigma Uhr which we subsequently obtained shows that this second notation was that originally intended by the Germans. From the point of view of their own security they made a great mistake in adopting the inferior method of starting off with the number encoded in the basic key as this at once drew our attention to the problem and told us that some transformation of the Jaguar stecker was the answer. If the Germans had adopted their prearranged system, the messages would have been considered dud and probably ascribed to a separate key. We would eventually have broken on a crib - when we had run a correct crib on a reciprocal Uhr - and then the connection with the basic stecker would have been noticed, but this might have taken a considerable time. It is at any rate clear that the Germans by departing from the explicit instructions of the devisers of this gadget greatly weakened its security value.

* For the Germans the Uhr substitution was determined automatically by the order of the stecker pairings on the key sheet. As we did not know this arbitrary order we had to break the Uhr apart from the basic key.

1·525 Summary

Enigma Uhr was a highly ingenious device and gave full entertainment value to the machine experts of Hut 6. It was regarded by the Germans as increasing markedly the security of the Enigma machine. It cannot be said to have done this in fact: but this was at any rate partly due to two mistakes of the Germans. Had they concentrated the use of Uhr more - e.g. had they made Jaguar, the key where they used it most, an all-Uhr key - and had they used the alphabetical notation from the start, they would have made out initial Uhr break much more difficult. As so often the Germans' piecemeal methods were their ruin. Yet even so Enigma Uhr remains a highly complicated and intricate device which yet does not from the security angle come within a thousand miles of the mechanically much simpler Reflector D.

In order to make Enigma Uhr a really dangerous device - something that would have upset our breaking technique - its basic principle of stecker transformation should have been carried further. The reader may care to consider what (for instance) would have been the effect of Enigma Uhr if the Uhr had been used in every message and made to move on one position for each letter encoded, thus giving rise to a cycle of forty stecker sets inside every message. Such a device would have necessarily involved radical changes in our bombe design, if not perhaps the invention of wholly new machines.

1·526 Appendix : Uhr Statistics

KEY	NO. OF UHR BREAKS	FIRST BREAK	LAST BREAK
JAGUAR	189	July 10, 1944	Apr. 9, 1945
CRICKET	39	"	Nov. 20, 1944
LILY	7	" 16, "	Aug. 24, "
SNOWDROP	18	" 17, "	Aug. 15, "
RED	31	" 22, "	Apr. 16, 1945
DAFFODIL	25	Nov. 18, "	Jan. 23, "
NARCISSUS	8	" 15, "	Nov. 22, 1944
LION	17	Dec. 2, "	Apr. 27, 1945
GENTIAN	1	" 29, "	Dec. 29, 1944
BEETLE	5	Jan. 21, 1945	Mar. 6, 1945
PUMA	2	Feb. 21, "	Feb. 27, "
ASTER	6	Mar. 2, "	Apr. 10, "
LEOPARD	2	Apr. 4, "	Apr. 6, "
MOTH	1	" 14, "	" 14, "
WASP	4	" 21, "	" 26, "
TOTALS	355	July 10, 1944	Apr. 27, 1945

1·53 GERMAN SECURITY DEVICES : ZUSATZ STECKER

1·530 The May Scare

In May 1944 the Germans introduced the most silly and trivial of their security devices: and yet the forewarning we received of their intention to do so caused considerable fluttering of the dovecotes in Hut 6. The reason was that the decode references to the impending change were from our point of view very cryptic: of course this was not due to intentional obscurities on the enemy's part but in the messages we intercepted and read he was merely making incidental references to documents not in our hands. What was abundantly clear was that on any one day three different sets of stecker were to be in use on one key: it was anybody's guess whether the sets were to be altogether different or whether the transformations would be effected by some predictable rule, as in the analogous case of the wheelorder change.

As always in doubtful circumstances, Hut 6 prepared for the worst, i.e. three completely different sets of stecker. This would mean that every key would have to be broken three times over indefinitely except that for the second and third breaks one would presumably know the wheelorder and ringstellung and could run on hoppity menus - which mean shorter cribs. This possibility was in one way providential as there were few if any keys where we could have produced every day in the relevant periods <u>three</u> full-dress cribs: but on the other hand we were faced with the necessity of a great expansion of our records as we might have to use as cribs beginners or signatures we had previously despised and hence left unrecorded. However, under the superintendence of the Qwatch, an enlarged scheme of records was set on foot and all embryo cribs were carefully noted.

1·531 A Damp Squib

What happened was indeed an anticlimax - though this was fortunate as the attempt to break three separate sets of stecker daily on every Air key would have lead to immediate bottlenecks in staff and bombes. As it is very doubtful whether we could at this late period of the war have materially added to our cryptographic staff, we might well have been faced with the dilemma of relaxing our efforts on the Air keys through sheer deficiency of staff or alternatively going full out on these keys by transferring staff from the Army side with consequent damage to the Army prospects. It is indeed fortunate that we were spared such a Procrustean choice.

The Germans took the following action - the stecker was changed at 0300, 1500, 2300 giving three stecker periods called by us R, S, T. In combination with the already existing wheelorder periods X, Y, Z the 24 hours from 0300 to 0300 we now divided into five key periods - 0300 - 1059 RX, 1100 - 1449 RY, 1500 - 1859 SY, 1900 - 2259 SZ, and 2300 - 0259 TZ.

Each set of stecker consisted as usual of ten stecker pairs plus six self-stecker but at 1500 one of the original stecker pairs was unsteckered and two of the originally self-steckered letters were steckered together. At 2300 the same process was repeated with another of the <u>original</u> ten stecker pairs and two more letters of the <u>original</u> six self stecker.

INFO
RECO

e.g. Red May 1, 1944

R A/E B/Y D/G F/J H/L K/O M/R P/U S/X T/V, C I N Q W Z

S A/E B/Y D/G F/J H/L L/Z K/O M/R S/X T/V, C N P Q U W

T A/E B/Y F/J H/L L/Z K/O M/R N/Q S/X T/V, C D G P U W

It is obvious that the alteration in the stecker is so slight that it is in general a fairly simple matter - with some knowledge of cribs or even without - to deduce the other two sets from any given set. Serious difficulty only arose when traffic in one period was very small: thus it was not always possible on certain keys to recover the T stecker. It is surprising that the Germans thought such a trivial alteration gave any additional cipher security worth bothering about. Still its nuisance value in R.R. D.R. and Watch/Research - for, after all, the changed stecker pairs had to be found - was not entirely negligible. The Machine Room gave great assistance in working out the stecker changes.

1.532 Extent of Change

The Army characteristically had nothing to do with this half-baked innovation but Zusatz Stecker was employed by all Air keys until about June 15th when it was dropped generally as suddenly as it came into use. Brown III which characteristically had been very slow to get the scheme straight - to begin with the Brown operators simply pulled out one end of a stecker plug and stuck it in somewhere else in an unoccupied hole - was equally characteristically the last key to use this trick, keeping it on to July 14th. The abandonment was hailed with jubilation by all concerned as Zusatz Stecker had become simply an annoyance and time-wasting nuisance, the more so as its solution had not the compensating value of demanding much cryptographic skill.

1.533 The German Idea

It is difficult to suggest any really satisfactory and adequate motive for the German introduction of this paltry nuisance. It may be suggested that it is in line with the remarkable German nervousness over depth (e.g. change of wheelorder) and in particular that it was introduced as a stop-gap until Enigma Uhr, a more radical stecker change idea, was ready. The whole conception, however, suggests the ignorance of the layman: Zusatz Stecker can scarcely have been born in the brain of a professional cryptographer. It is not improbable that the Germans themselves gave it up in disgust, eventually realising that such a futile key-change was not even worth the trouble it caused to their own operators.

V W
INFC
RECC

1·54 GERMAN SECURITY DEVICES : NOT SCHLUESSEL

1·540 Introduction

The use by the Germans in certain circumstances of Not-schlüssel (Emergency keys) is as a security measure not quite in the same category as those already discussed. The object was not to render cryptography more difficult but to give a quick method of distributing new keys in case of compromise, particularly to isolated garrisons. The method adopted was to devise a system by which an Enigma key could be generated by a single keyword while the discriminant was found from another word. The two words could be selected from an emergency list held in reserve or in case of need sent over the air in Enigma. This last procedure was actually most insecure as we had captured the German instructions and so could devise the key from the key word as well as they could: but this knowledge was hidden from them.

1·541 First System

The first system used by the Germans was in fact employed wholly by the G.A.F. so far as we know. It was explained in two documents that came into our hands in the middle of August 1944. The proc-edure is best described by an example.

Let the keyword (Schlüsselwort) be OSTSEEFISCH*. We first strike out all but the first example of any repeated letter giving the "fillet" OSTEFICH. We then write underneath this fillet in alphabetical order all the other letters of the alphabet thus:-

6 7 8 2 3 5 1 4
O S T E F I C H
A B D G J K L M
N P Q R U V W X
Y Z

and (as shown) number the letters in the fillet alphabetically. We then read off the letters by columns, in the numbered order, and arrange them to form a rectangle 13 x 2, thus:-

C L W E G R F J U H M X I
K V O A N Y S B P Z T D Q
4 1 5 2 3

We number from 1 to 5 the five letters in the bottom row that come earliest in the alphabet and then read off the key thus:-

Wheelorder: 4 1 5 (the first three numbers from the left)
Ringstellung: C E G (the letters of the top row above those numb-ered letters that give the wheelorder)
Stecker Pairs: L/V W/O R/Y F/S J/B U/P H/Z M/T X/D I/Q

It should be noticed that all the normal key rules disappear; in particular, consecutive stecker are possible. There is, however, one way of identifying a broken key as NOT - the(German) rings-tellung involves letters that are self-steckered. (This can be used as a short cut to the ringstellung of a NOT-key).

The discriminant of a NOT-key is obtained from the Kenn-gruppenwort by using the 1st, 3rd and 5th letters: there is thus only one discriminant a key and stutterers are quite possible.

* C H, C K are <u>not</u> to be replaced by Q: also an umlaut is ignored.

INFO
RECC

1.542 First Appearance of the NOTS

These emergency keys were first used towards the end of August when a number of unidentified discriminants - notably TAS, ASH, TEN - appeared on the Snowdrop frequency 4560. Some of these turned up on more than one day but when E/4560 was broken on a R.E. only the messages with the discriminant ASH decoded. Nigel Forward was able to demonstrate that the key was the first of the NOTS by deducing the generating word NORDLICHT. The key was named E/NOT/ASH and this and all later NOT-keys were entered in a special NOT keybook ✱.

1.543 The Saga of Guernsey or the Qwatch and the Forty NOTS

Now we arrive at the great NOT period. From the beginning of September 1944 onwards Row 70 of the Jaguar star A began using NOT-keys. This row was used by the unfortunate "General der L.W. Kanalinseln", whose H.Q. was in Guernsey and who was now completely cut off. He had no regular key and could not get one; hence his constant use of emergency keys. A list of the discriminant cycle from September 1 to October 10 is inserted herewith: the discriminants from September 1 to 5 are bracketed as no traffic was actually passed on these keys but it is known that these are the discriminants that would have been used.

Sept.	1	(OEN)	Sept.	21	FIC
	2	(TAE)		22	KSM
	3	(PED)		23	LPO
	4	(KKO)		24	EHB
	5	(TAS)		25	BHS
	6	TBK		26	DEK
	7	ASH		27	TCR
	8	TEN		28	TIH
	9	IRE		29	ERH
	10	DNN		30	TAC
	11	HSL	Oct.	1	HSL
	12	ASR		2	ASR
	13	TBK		3	TBK
	14	BGE		4	BGE
	15	NBN		5	NBN
	16	PRE		6	PRE
	17	NRL		7	NRL
	18	OTE		8	OTE
	19	NLO		9	NLO
	20	DNN		10	RNG

In this unimpressive list of trigrams is locked the secret of the forty NOTS. The keywords from September 8 to 10 were given us as follows:-

	Schlüsselwort	Kenngruppenwort
8	Ostseefisch	Trennschnitt
9	Nimrod	Harfe
10	Randgebiet	Duenenlandschaft

and this was the beginning of our building up of the series of forty code words. Some other keys were also broken on R.E.'s and NOT/ASH with its code word NORDLICHT was already known.

✱ The reason for this was that in principle NOT-keys were independent of date and our normal keybook was arranged by date. However, the NOT Guernsey keys did change daily and were usually entered in our regular keybook as well as in the special NOT keybook.

INFC
RECC

From now on the position got steadily more complicated. First, it became clear that the "one discriminant, one key" theory was not universally true. It will be noticed that up to September 30 there are two cases of repeated discriminants in the list, viz. TBK on September 6 and 13, DHN on September 10 and 20. Now on September 10 and 20 the same key decoded all the traffic: it did not decode anyone else's TBK traffic nor even Row 70's traffic on September 6. It was fortunately possible to disprove the theory that the key E/TBK had been worked out wrongly by the Germans for we were able to recover the generating word PFERDEKOPPEL (= paddock)

In October the mystery deepened. As will have been noticed the discriminants from October 1 - 9 repeat those from September 11 - 19 but the October traffic did not come out on the September keys, several of which had been broken. Fortunately we were quickly able to break NOT/GUERNSEY of October 4 on a R.E. from Raster[x] and the key was found to be completely different from the NOT/BGE key used on September 14.

Once again we tried to break the keyword and soon arrived at the fillet ENHOBAK which did not look like any German word. However, about the same time there was a somewhat obscure message finally translated as follows:-

"Key message from 1/10 0300 hours
Kenngruppenworte as Schluesselworte, read backwards, beginning with Laufende Nr.1. Kenngruppen from the Schluesselworte, read forwards."

With this hint of reading backwards we reversed the fillet to read KABOHNE. This suggested KAKAOBOHNE which read forward gave the fillet KAOBHNE (which generated the key of September 14) and read backwards the fillet ENHOBAK[θ] (which generated the key of October 4). Also KAKAOBOHNE is clearly one of the original discriminant words - see KKO on September 4.

It was by this time clear that the General had been given a list of ten pairs of code words which he had used straight from September 1 to 10 and afterwards in several varied ways. It is possible to derive forty keys from ten pairs of words by using each word in turn as the keyword and using it first forwards and then backwards. The General's scheme was soon discovered to be as follows, if we denote the original Schluesselwort by S and the original Kenngruppenwort by K:-

	Schluesselwort	Kenngruppenwort
Sept. 1 - 10	S forwards	K forwards
" 11 - 20	K forwards	S forwards
" 21 - 30	S backwards	K backwards
Oct. 1 - 10	K backwards	S forwards
" 11 - 20	S backwards (from no. 10 to 1)	K backwards

It was possible to deduce the scheme up to October 10 from the keys already broken; and the scheme from the 11th to the 20th was given to us in a message of the 10th.

x The General had a Raster key which he continued to use in happy ignorance of the fact that it was already at the Park.

θ Note that the fillet from a backward word is not necessarily a backward fillet.

INFC
REC'

It will be seen that only forty keys are possible and are all used in the period September 1 to October 10: so, in order to have NOT/GUERNSEY out until the General got a new set of words, we had merely to find the forty code words. A number were already known by analysis from the keys and from source: but the attack was now pressed forward more systematically under the guidance of the Qwatch. It was now much easier to find the keyword for broken keys for in every case we could say "The discriminant formed from the keyword for which we are looking is (say) TAE: therefore the word is T.A.E..." In this way keyword after keyword was discovered and more and more keys written out.

It was also possible to discover keywords even when the key had not been broken. For example, on 25/9 the discriminant was BHS and on 5/9 TAS. Hence the generating word must be T.A.S..... S.H.B., the central dots representing an unknown number of letters. Another skeleton crossword clue was A.S.H.....R.C.T. Both of these were solved by fortunate inspirations and the aid of dictionaries* and in short we were ultimately successful in hammering out the complete list which is inserted herewith.

Final list of Keywords and Discriminant Words

Lfd. Nr.	SCHLUESSELWORT	KENNGRUPPENWORT
1.	HASELRUTE	OZEANSCHIFF
2.	ANSTRICHFARBE	TRAUERMUSIK
3.	TABAKPFEIFE	PFERDEKOPPEL
4.	BAGGERSCHIFF	KAKAOBOHNE
5.	NEBENHAUS	TRANSPORTNACHSCHUB
6.	PFRIEM	TABAKFELD
7.	NORDLICHT	ANSCHAUUNGSUNTERRICHT
8.	OSTSEEFISCH	TRENNSCHNITT
9.	NIMROD	HARFE
10.	RANDGEBIET	DUNENLANDSCHAFT

It will be noticed that this list clears up the mystery of the two E/TBK keys referred to above as there are two words that give the discriminant TBK.

It is perhaps worth noting as a minor point that, while the key derived from a word written backwards is in general quite different from the straight key, in certain special cases there is a good deal of similarity. One such is when the keyword has six different letters and the column numbers differ by three on columns 1 and 2, 3 and 4, 5 and 6 (reading from left to right). An example is the word PFRIEM where the similarity of the two 13 x 2 rectangles is noteworthy.

e.g.

5	2	6	3	1	4
P	F	R	I	E	M
A	B	C	D	G	H
J	K	L	N	O	Q
S	T	U	V	W	X
Y	Z				

4	1	3	6	■	5
M	E	I	R	F	P
A	B	C	D	G	H
J	K	L	N	O	Q
S	T	U	V	W	X
Y	Z				

E	G	O	W	F	B	K	T	Z	I	D	N	V
M	H	Q	X	P	A	J	S	Y	R	C	L	U
	3				1	4			2	5		

E	B	K	T	Z	F	G	O	⁄	I	▯	▯	▯
M	A	J	S	Y	P	H		X	⁄	▯	▯	▯
5	1	4				3				2		

* For the answers see nos. 5 and 7 in the list below.

INFO
RECD

giving the keys:- 314 GBK C/D E/M F/P I/R L/N O/Q S/T U/V W/X Y/Z

and 514 EBK C/D F/P G/H I/R L/N O/Q S/T U/V W/X Y/Z,

with two wheels, two ringstellung letters and nine steeker pairs in common :

To conclude the Guernsey saga we should give an example of the method of deriving the keyword from the broken key. The following example was broken with no information as to the word: later normally three letters of the word were known which is naturally a great help. The general process is a mixture of logical deduction plus trial and error.

Example Given a key, to find the keyword.

NOT/ASH 451 AVC (German CYD)

B/H E/I F/Q J/U K/W L/P M/S O/V R/Z T/X
A C D G N Y.

We must have C Y D
G N A
4 5 1

Hence no letter between G and N is on bottom line, so that H I J K L M / B E U W P S are all that way up. This fixes B as 2, E as 3 and makes $\frac{H}{B}$ and $\frac{I}{E}$ to the right of $\frac{D}{A}$ in the 13 x 2 block. Also from the numbering $\frac{F}{Q}$ is that way up. Now A, B, E are not in the word (or they would be in the top row in the 13 x 2 block) and if D is, it is not the first letter alphabetically, i.e. if D is, C is also. From our knowledge of German it is almost certain that if C is, H is also: let us suppose as a reasonable guess that C and H are both in the word. The letter preceeding A in the 13 x 2 block must be in the word: if there is nothing between $\frac{Y}{N}$ and $\frac{D}{A}$ this letter is N which is by no means improbable. If we are right so far, D is in the word: otherwise Y, an unlikely letter would be. Thus (bracketing letters known to be in the word) we now have as our skeleton for the 13 x 2 block $\frac{(C)}{G}$ $\frac{Y\ (D)}{(N)\ A}$ (H) B.

Now what is to follow D? A, B, C, G, H are impossible from the figure and E because $\frac{I}{E}$ are the right way up. F is the first possibility we come to and we know F is in the top row; also (N) A Q is a reasonable collection as A must begin the second row of the original block and Q is about where we might be in the last

row. So let us try

	(C)		Y	(D)	F		(H)
	G		(N)	A	Q		B

The letter after B must be soon after Q in the alphabet: it cannot be R which would imply (H) Z - impossible. Let us try S: this implies that R is in the word and we observe a good place for (R) is after S which gives the plausible combination (H) M Z on top, thus:-

(C)	Y	(D)	F	(H)	M	Z			N			D		C	H
							and	A	B	E	F	G		M
G	(N)	A	Q	B	S	(R)			Q	S				Y	Z

C and H coming together is equivalent to a confirmation !

The rest is easy. From the second diagram the original fillet must be nine letters, so there are two more columns to be filled in apart from the obvious spaces. We must have

N	?	?	D	?	?	C	H	?
A	B	E	F	G	?	?	M	?
Q	S	?	?	?	?	Y	Z	

We know R is in the word and <u>one</u> of the letters T U V W X must be: T and U are the most likely. Two of I, J, K, L are also in the word and one of O P. I C H seems irrestible and we see the light ! The answer is N O R D L I C H T.

The completed blocks are as under:-

6	7	8	2	5	4	1	3	9
N	O	R	D	L	I	C	H	T
A	B	E	F	G	J	K	M	P
Q	S	U	V	W	X	Y	Z	

(C)	K	Y	(D)	F	V	(H)	M	Z	(I)	J	X	(L)
G	W	(N)	A	Q	(O)	B	S	(R)	E	U	(T)	P

While hardly falling under the category of machine cryptography, exercises of this nature were a pleasant pastime for Hut 6 and by no means of academic importance as has been shown. It should, perhaps, be mentioned that the above example is as it happens easier than the general run.

1.544 The Plague of NOTS

NOT/Guernsey was regularly broken up to the end of the year and on a few days later: the General incidentally eventually got a new set of codewords, but kindly told us how he intended to use them, so the cryptographic interest was ended. The G.A.F., however, continued to use this NOT-system whenever necessary: in particular from January 12 to 16 a perfect plague of NOTS raged on the Ocelot system during a compromise. No fewer than 24 NOT-keys were broken mostly on R.E.'s: in few, if any, was an attempt made to find the keyword as this was an academic exercise when there was no reason to suppose that the word was going to be used again.

INFO
RECD

1.545 NOT-keys, New Style

In December 1944 the Germans gave in a document entitled "ANLEITUNG ZUM ABLEITEN DES NOTSCHLUESSELS FUER DIE SCHLUESSEL-MASCHINE ENIGMA" full details of a new style of NOT-keys. This was definitely an improvement: a pair of code-words gave keys for a month, and yet there was perfect security, as the codeword is virtually unbreakable from a given key. The following is a translation of the document:-

N O T S C H L U E S S E L

1. What it consists of:-

The Notschlüssel consists of two key words (Lösungswörter) of different lengths. From the longer, the Schlüsselwort, are deduced machine set-ups which change from day to day, and from the shorter, the Kennwort, is deduced the Kenngruppe.

2. Period of validity

The same Lösungswörter (i.e., Schlüsselwort and Kennwort) are to be used for not more than 30 days, including the day when they first come into force. Its use may be continued over the end of the month in which it is issued within the limit of 30 days. A Notschlüssel which has come into force should as soon as possible be replaced by an Ersatz Schlüssel.

3. Choice of the Lösungswörter

The Schlüsselwort must be at least 12 letters long. The Kennwort must be at least 5 and should at the most be 10 letters long.

Both Lösungswörter should be part of the normal vocabulary of the Funktruppführer and should admit of no ambiguity in spelling. In the Lösungswörten ch and ck should not be replaced by q; similarly j should not be replaced by i. ä, ö, ü should be written ae, oe, ue. The two Lösungswörter should have no affinity of meaning (e.g. Strassenbahn, tramway, and Schaffner, conductor). There should be no limitation to a particular class of word in their choice (e.g. Nouns).

4. Process for the deduction of the Notschlüssel

From the Schlüsselwort a machine-setting (Wheelorder, Ringstellung, and Stecker) is constructed. This is called the Hilfsschlüssel.

A table in the lid of the Enigma gives 31 different Grundstellungen for the different days of the month.

With the Enigma set up according to the Hilfsschlüssel and the Grundstellung, the Schlüsselwort must be tapped out four times. From the resulting succession of encoded letters (different every day), the Notschlüssel (Stecker, Ringstellung and Wheelorder) is constructed. Considered separately, the Hilfsschlüssel and the Notschlüssel are constructed in the following way:-

INFC
REC'D

5. Construction of the Hilfsschlüssel

Wheelorder. Always 1 2 3 *

Ringstellung. Last three letters of the Schlüsselwort.

Stecker. The different letters of the Schlüsselwort, in their order in the Schlüsselwort, are collected in pairs from the beginning of the word, provided that in the process new and consistent pairs result. These pairs are to be steckered. If there are less than 10 pairs, the stecker process should not be extended to the customary 10 pairs.

Uncle D. If used, always to be alphabetically plugged:

AB CD EF GH IK LM NO PQ RS TU VW XZ

6. Grundstellung

Fixed Table in the lid of the Enigma:

1	2	3	4	26	27	28	29	30	31
01	02	03	04	26	01	02	03	04	05
01	02	03	04	26	02	03	04	05	06
01	02	03	04	26	03	04	05	06	07

Use of the Table

Look for the number of the day of the month in the first row of the table. The three numbers underneath are the Grundstellung for the encoding of the Schlüsselwort.

7. Construction of the Notschlüssel

The Hilfsschlüssel and Grundstellung to be set up according to para. 5 & 6 and the Schlüsselwort tapped out four times.

8. From the succession of encoded letters obtained according to para. 7 the following is deduced:

Stecker:

Different letters in succession are to be steckered together. Therefore the letters in the given order should be immediately steckered; the first three letters which occur more than once and are therefore no longer "steckerable" are to be ringed round. If there are less than 10 pairs, the stecker process should not be extended to the usual 10 pairs, but only the existing pairs are to be steckered. If there are ten or more pairs, the first ten should be steckered. If there is an uneven number of different letters the last of these is to be ignored.

Ringstellung:

The first three repeated (ringed) letters.

Wheelorder:

The last five letters (corresponding to the number of wheels) are to be numbered 1 to 5 according to their position in the

* On the evidence of a prisoner of war this rule has been superseded and the wheelorder now changes every three days.

INFC
REC'D

alphabet. If a letter occurs more than once the numbering is done according to the position of the letters within the five-letter group:-

e.g., a m c m p
1 3 2 4 5 = wheelorder

The last three of these numbers gives the wheelorder.
Uncle D; if used, always alphabetically plugged: AB CD EF GH IK LM NO PQ RS TU VW XZ

9. Kenngruppe

The first, third and fifth letters of the Kennwort form the Kenngruppe. The Kenngruppe does not change daily but remains the same as long as the Notschlüssel remains valid. It is to be used as seldom as possible.

10. If it is necessary to write down the key deduced, each letter of the pair should be put in alphabetical order and then the pairs written down in alphabetical order according to the first letter of the pair. All other workings involved in the deduction of the Notschlüssel are to be destroyed without a trace.

EXAMPLE (illustrating preceding paragraphs).

1: Notschlüssel

Landerziehungsheim (= Schlüsselwort)
Rutschen (= Kennwort)

2: Notschlüssel for March is used from 27th March to 9th April (in any case not after 25 April)

5: Hilfsschlüssel:

Wheelorder: I II III
Ringstellung: EIM = 05 09 13

Stecker:

L A N D E R Z I E H U N G S H E I M

LA ND ER ZI HU GS HM

6: 28.3.45 = Date 28
Corresponding Grundstellung 02 03 04

7:

L	A	N	D	E	R	Z	I	E	H	U	N	G	S	H	E	I	M
z	o	m	(m)	a	p	j	v	d	(p)	l	r	k	(m)	f	t	k	k
f	t	m	c	n	s	o	o	g	x	d	c	u	m	r	a	l	x
c	s	g	x	g	f	c	d	g	t	o	m	x	f	t	g	o	t
m	j	d	r	k	v	x	t	d	r	l	u	v	a	m	c	m	p

(Cipher text invented)

8: Stecker:

ZO MA PJ VD LR KF TC NS GX BQ

Ringstellung: (ringed in the example):

(m) (p) (m) = 13 16 13

Wheelorder:

a m c m p
1 3 2 4 5 = II IV V

9: Kenngruppe:

r u t s c h e n
r t c

10: AM CT DV FK GX JP LR NS OZ

It will be seen that it is (unless one is extremely fortunate) impossible to deduce the Schlüsselwort from the key and so generate the remaining keys: also that keys so made up are unrecognisable externally except for the unchanging discriminant (which is to be used as little as possible) and the chance that they may have less than ten stecker pairs. The scheme was not, so far as we know, used by the G.A.F: to the end their NOTS were of the original type. But one Army key NOT/AFE was of this class, as the discriminant lasted for about a month. The key was broken on March 19 and was

234 XDP B/Y D/W F/S G/V K/N L/P M/O Q/Z R/U T/X, A C E H I J
(German)

If he relishes the task, the reader is invited to beat Hut 6 by finding the codeword !

One peculiarity about this new system should be mentioned. It will have been noticed that provision was made for D - and the NOT D was duly entered as D 307 in our records. But it is clear that on a mixed B and D key construction of the NOT-key as directed means that the key as used with B and as used with D will be different. This can hardly have been intended: either it it is an oversight or the compiler disregarded the possibility of mixed keys, taking it for granted that a NOT-key would be all-B or all-D.

1.546 Conclusions

The two systems of constructing NOT-keys were equally ingenious: the second is preferable from the point of view of security, as it gives a month's keys from a pair of words while keeping the codewords inviolate.

These systems were only intended by the Germans for use in emergency. However, NOT-keys have actually certain advantages over keys made up in the normal way owing to their freedom from rules of keys which may help the enemy cryptographer. They would have, however, the fatal objection for regular use that if the actual key is generated from one word the number of possible keys is limited so drastically that some kind of key index becomes possible - for instance, on the second system the number of keys is determined by the number of German words at least 12 letters long - which must surely be much less than 100,000.

V W
INFO
RECC

It would appear then that the regular use of any system of deriving keys from key-words could never be secure unless two conditions were satisfied:-

(1) that the method adopted did not, in itself, give rise to any peculiarity or rule in the keys;

and (2) that the number of possible keys was not substantially reduced by the method of derivation; and in practice to satisfy the second condition it would be necessary to derive each key from more than one keyword.

INFO
RECC

1·55 OTHER GERMAN SECURITY DEVICES

1·550 CY

First Introduction About the middle of September 1944 a new German security device was noticed, first of all on a few Jaguar and Barnyard links. A number of messages were observed to go off into nonsense in the middle and it was quickly noticed that this always happened just after the decode read CY followed by two consecutive letters, e.g. RS. It was soon discovered that the rest of the message could be decoded if immediately after CYRS the left-hand wheel was set to the first of the two consecutive letters (in this case R). Of course, the consecutive letters were not always the same, but the CY was invariable.

Extension of the Practice Apart from the Jaguar messages already referred to - and these were very few in number-CY was purely an Army idea and it spread fairly quickly to all Army keys and also the S.S. keys. Indeed it was later discovered that the Police key, Roulette, was the first key to use CY, as the device appeared in one early September day that came out rather late. By October CY was in practically universal use on all Army and S.S. keys except on short messages. (The reason for this exception will appear later).

The German Regulations In October 1944 we captured a German document entitled "Anderungen bei Schlüsseln mit Maschinenschlüssel". The second section of this document dealt with CY and a translation follows.

B. Resetting wheels within messages

1. The cipher clerk will interrupt the enciphering of the text of the message in all messages of 150 - 250 letters* once between the 70th and 130th letters, e.g. at the 93rd letter.

2. The interruption will occur at a place chosen at random. In no circumstances may the interruption take place regularly at the same place, e.g. the 100th letter, or always at the end of a 5 letter group. It is recommended to introduce it at the end of a word or sentence of the Klartext.

3. After interrupting the enciphering the cipher clerk will read off the position reached at the left-hand wheel, e.g. 21, and will choose at random, without at first altering the positions of the left-hand wheel, a new position which must be at least 5 stages removed from the position reached.

4. The cipher clerk then establishes in the usual manner which letter corresponds to the new value, e.g. 06 = F. He will then encipher, still without previously altering the position of the left-hand wheel, first as a "Weisergruppe" CY and then the letter showing the new value and the letter immediately following it alphabetically, in the example F and G; he will add the four resultant enciphered letters to the cipher text so far written out.

5. The cipher clerk will then set the left-hand wheel at the new position (in the example 06 and will continue to encipher the message in the usual way.

* 250 letters was the length limit for German Enigma messages. This regulation at least was well observed.

SECRET
INFO

6. In deciphering the reverse process is to be carried out. Messages or message parts with a length of 150 messages or more are to be given particular attention between the 70th and 130th letters. Should the "Weisergruppe" CY appear, deciphering is to be stopped after tapping out the next two letters of the cipher text. The "clear" letter after the Weisergruppe CY is to be converted to a two figure number in the usual manner; the left-hand wheel is to be set at this number and the deciphering continued.

These German regulations were ordered to come into force on September 15, 1944 and on the whole were strictly obeyed by the Army. Occasionally CY would be omitted in a long message or used in a message less than 150 letters long.

Effect on Breaking The most important result of CY was that it effectively ruled out cillying which was now (if it occurred at all) very hard to spot. Whether from this cause or from the concomitant introduction of random indicators, cillying virtually ceased on Army traffic and S.S. keys - a loss that would have been more serious had not cillies already been very rare (except on Orange).

Other difficulties were that the insertion of the four dummy letters at an unknown spot upset cribs - particularly top and tail shots - and more especially re-encodements. Of course it was a help to us to have the German regulations so that we knew when to expect CY and most cribs did not run into the danger zone. Greenshank R.E.'s were especially affected, as (because of the presence of D) it was necessary to write out at the very least 80 letters correctly and (even apart from CY) this was by no means easy (see the Theory of Re-encodements in the technical volume.) Yet it is surprising how often these difficulties were overcome, and the position of CY fixed, at least approximately.[θ] On the whole, while a distinct nuisance to the investigator of R.E.'s, CY did not overthrow our matured technique.

In one minor aspect CY was an advantage. It provided on occasion - particularly when a day came out on the beginning of a message - a short cut to the ringstellung which was often taken advantage of by Army cryptographers.[+]

Conclusion CY is probably best thought of as a device for removing (if only to a slight degree) one of the main theoretical defects of the Enigma - the extreme regularity of its wheel motion. In default of a mechanical method of producing a more irregular motion[Z] the idea of breaking the continual uniformity by an unpredictable change once in each message is not without merit though it is essentially only a makeshift.

θ Sometimes exactly because of the usual tendency to insert CY after a break in the sense (see regulation 2 in the German document).

+ If CY had been widely used on Air keys it would have increased the difficulty of breaking an Uhr substitution on a dottery.

Z The Germans had planned to introduce this later - see the closing chapter of this book.

SCRA INFO RECS

1.551 Random Indicators

The Regulations The German document referred to in the last section contained in its first half regulations for the security device Hut 6 named "Random Indicators". It will be convenient to quote the salient parts of this document.

A. Choice and use of the Indicator (Spruchschlüssel)

I. Definitions

1. The six letters inserted in the preamble of a message enciphered with Enigma after the number of letters or as the case may be after the discriminant group denote (according to H.Dv.g.14 - "Introduction to cipher machine Enigma") the "Grundstellung" and the "Spruchschlüssel", previously chosen at random by the cipher clerk. In the following instruction terms will be used as follows:-

(a) "Grundstellung" has the same meaning as hitherto.
(b) "Spruchstellung" will replace what has previously been called "Spruchschlüssel".
(c) "Spruchschlussel" will denote "Grundstellung" and "Spruchstellung" together.

2. The "Spruchschlüsselliste" contains the "Spruchschlüssel" for one day. It is to be made up by the Funkleiter or his deputy (Funktruppführer). It changes daily at 0300 hrs.

II. Procedure for arriving at the Spruchschlüssel

3. The Funkleiter or his deputy must

(a) choose a random Klartext of general content (texts from books, songs, letters etc., but not texts of service or official content).

(b) set a cipher machine Enigma as follows:-
(aa) Wheelorder: I II III
(bb) Ringstellung: 01 01 01
(cc) Stecker connections: 10 stecker connections, chosen completely at random, are to be plugged.
The stecker connections of any day's key must not be used.
(dd) Grundstellung: at random, e.g. 13 07 21.

(c) The Klartext chosen according to (a) is to be tapped out on the cipher machine set according to (b). The resultant enciphered letters are to be entered in the Spruchschlüsselliste consecutively in groups of six letters. Each group is a Spruchschlüssel. As many groups are to be obtained as will cover the daily requirements in Spruchschlüssel.

III. Spruchschlüsselliste

4. Spruchschlüssellisten are to be prepared in duplicate; they are to be marked with the date of compilation and signed by the compiler.

5. The Spruchschlüsselliste is in general to be compiled daily. It is, however, permitted to compile Spruchschlüssellisten at slack times for several (at the most ten) days in advance. These are like cipher instructions to be kept by the Funkstelle-

SECRET
INFO
M 1

arbeiter who will issue a new list daily to the Funkleiter.

6. The original of the Spruchschlüsselliste is to be handed to the cipher clerk shortly before the change of the daily key. If it is handed over earlier it must be in an envelope or otherwise sealed. The envelope may only be opened by the cipher clerk shortly before the change of the daily key.

7. The second copy of a Spruchschlüsselliste is to be handed by the compiler to his immediate superior immediately after completion. In a duplicate copy the stecker connections, the selected Grundstellung and Klartext used to obtain the Spruchschlüsselliste must be detailed.

e.g. Duplicate copy of Spruchschlusselliste No. 10.

Stecker connections: KC GO RX DA MP TW HB LN SF VZ
Grundstellung : 13 07 21
Klartext : Gottfried Keller, der gruene Heinrich, S.23, Absatz 2 ff.
(Sgd) Meier, Wachtmeister and deputy Funkleiter.

8. Should all the Spruchschlüssel not be used up on the day for which the Spruchschlüsselliste has been compiled, those not used can be taken over unchanged in the Spruchschlüsselliste of another day. In this case it must be clearly shown (in coloured pencil) on the duplicate copy of the Spruchschlüsselliste which Spruchschlüssel have been taken over and from which Spruchschlüsselliste.

9. On receiving the duplicate copy the station, which monitors the W/T station concerned, is to carry out frequent tests to see whether the compilation of the Spruchschlüssel and its use is in accordance with the regulations.

Offences are to be dealt with by taking disciplinary action.

IV. Handling the Spruchschlüssel

10. In enciphering

(a) Set the Enigma on the new day's key.
(b) Put the 1st Spruchschlüssel (= 1st six letter group of the Spruchschlüsselliste) at the head of the message (part) to be enciphered.
(c) Set the Enigma at the Grundstellung (Grundstellung = three letters at the right of the Spruchschlüssel).
(d) Tap out the Spruchstellung, (Spruchstellung = three letters at the right of the Spruchschlüssel).
(e) Set the Enigma at the three letters resulting from tapping out the Spruchschlüssel.
(f) Encipher the message.
(g) Delete the Spruchschlüssel employed from the Spruchschlüsselliste.
(h) On the message pad note the number of the Spruchschlüsselliste (No. = date).

11. The next Spruchschlüssel in order is to be used for each message (part) to be enciphered. In no circumstances may one and the same Spruchschlüssel be used again.

INFO
RECC

12. In deciphering

(a) Enigma to be set at the day's key of the message to be deciphered.
(b) Set the Enigma at the Grundstellung in the preamble of message to be deciphered.
(c) Tap out on the Enigma the Spruchstellung in the preamble of the message to be deciphered.
(d) Set the resultant letters on the Enigma.
(e) Decipher message.

Extension of the System It will be noticed that (as opposed to such devices as CY) there is no external indication of the use of the system of random indicators but from various small scraps of evidence it seems not unlikely that it was used fairly extensively, at least on Army and S.S. keys. The evidence is:

(1) these keys used CY punctiliously and thus might be expected to use the companion devices;

(2) the sudden cessation of cillies on Orange and (to a lesser degree) Roulette is most easily explained by random indicators (in the case of Orange at least CY is not adequate in itself: in August 1944 long strings of keyboards had appeared and the use of CY will not conceal an absolutely first-class cilli story though it will camouflage a weak one);

(3) the fairly frequent use of repeated indicators on Army keys is best explained by inadvertent breaches of rule 11 (caused one imagines, by an omission to delete a used Spruchschlüssel);

(4) the actual use of the device is proved by the capture of at least one enigma set up with wheelorder 123, ringstellung AAA (German) - see paragraph 3(b) - and by the later capture of more than one Spruchschlüsselliste.

Conclusion It is impossible to interpret "Random Indicators" as anything but an anti-cilli device - a far more radical one than CY. It does indeed kill cillies and it is clear that the Germans had at last become conscious of this possible danger. The answer they now found to the danger of cillies was as effective as anything that could have been devised - short of a complete change of the indicating system - and it did lose us Orange. The only possible criticism we can make of the German action is that (as so often) it was too late: cillies were dying when they were killed. The history of Hut 6 would have been different had the Germans in the full flush of their 1940 triumphs been able to spare a thought for the suppression of cillies.

1·552 Wahlworts

Introductory. A wahlwort[+] may be defined as a word chosen at random by the encoder of a message and placed at the beginning or end for the sole purpose of defeating enemy cryptographers. This particular device has a long history prior to 1944 which it will be convenient to retrace now.

The first occurrence of wahlworts was on the African Army keys (the Finches) in December 1942. Early in that month the Germans sent in Chaffinch a strong anti-crib warning to the effect that (1) addresses and signatures were to be buried in messages, preceeded by a warning signal e.g. "Here follows address" and (2) addresses (if of standard length) were to be altered by the

[+] The German word quickly became naturalised in Hut 6 parlance and the attempt to introduce "nonsense word" as an English equivalent never caught on.

prefixing of nonsense words. Long before the month was out the second instruction had been carried into effect (the proviso being disregarded) and a plague of wahlworts had infected all the African keys with the providential exception of Phoenix.

The effect on the breaking position was immediately serious, but this is discussed more fully in the history of the keys concerned. This first great wahlwort crisis was possibly not in itself much worse than subsequent crises on other colours but for two reasons it produced a much greater impact on the Hut as a whole. Firstly, the colours concerned were among the most important operational keys being then broken and they could not be laid aside if necessary (as could be done to a certain extent with wahlwort-ridden keys later on) and hence the increased bombe time they required had an immediate effect on the fortunes of other keys: and secondly, our bombe resources were still so limited that a prolonged crisis of this nature might (and at its worst moments did) almost rule out running of Research jobs altogether, a result that would not have been arrived at had a similar crisis recurred a year later when we had more bombes here as well as American resources.

Extension of Wahlworts Wahlworts were never used on S.S. keys and until the closing months of the war were mainly an Army device. It is a little difficult to describe their extension in terms of keys both accurately and briefly, as there were many fluctuations and throughout their use depended entirely on individual encoders' habits; thus it must not be imagined that when it is stated that a certain key at a certain time used wahlworts this necessarily means that every message on the key had a wahlwort. The cryptographer had to consider each individual case on its merits and try to assess on the latest available evidence whether the particular crib message on which he was working was likely to have a wahlwort or not. But in what follows we cannot do more than trace this extension in the most general terms. To consider Army keys first, from December 1942 to the end of the campaign in May 1943 wahlworts were freely and widely used on all African Army keys except Phoenix. But during the rest of 1943 it became clear that in theory at least the use of wahlworts was a general Army security measure. There was hardly any Army key that might not use wahlworts, though there were at this stage few that employed them as thoroughly as the African keys had done.

However, to cite examples, Raven used wahlworts in May, Buzzard, Cormorant and (to a lesser extent) Albatross in June, while Vulture (pronounced free of the plague in July 1943) had succumbed when the next break was made in August. In autumn 1943 and early 1944 wahlworts appeared on Bullfinch, Shrike and even Sparrow, which had originally been free of the nuisance. Wryneck (another victim of the epidemic) had on the Rundspruch, one of its principal cribs, an interesting cycle which shows how everything depended on the encoder's habits. On day 1 the crib started and finished flat, i.e. without wahlwort or even signature and address: on day 2 it began with a wahlwort followed by the address and ended with a signature possibly followed by another wahlwort: finally, on day 3 the crib began with wahlwort, address, signature and ended flat.

In the last year of the war wahlworts were very fortunately not used to a predominant extent on Western Army keys with the exception of the general key Puffin. (O.K.H. who used wahlworts regularly was particularly liable to speak on Puffin). But on the other hand the Eastern and Balkan keys became more and more

INFO M

addicted to wahlworts; in fact Avocet surpassed all other keys in consistency and thoroughness in this respect. Thus it may be said that by the end of the war wahlworts were fairly universal on Army keys; Greenshank, however, was to the end a distinguished exception.

A few Air keys used wahlworts from an early date. Locust, for example, impaired the value of its excellent crib, the Synoptic Weather, by prefixing wahlworts in April 1943; and at the same time Mustard, the key of the German Y service - a point not without significance - introduced the same device. Mustard remained faithful to wahworts ever after and in fact in a short paper on Mustard written in March 1944 this was selected as one of the general characteristics of the key. While in this case the introduction of wahlworts did not shake off our hold completely, breaking certainly became more intermittent; and it was not until 1944 that the situation was again satisfactory.

Apart from these exceptional cases Air keys generally remained free of wahlworts until the closing months of the war. (The occasional use of nonsense words to fill up tuning messages is closely analagous to the wahlwort proper, but these messages are a special case). But from December 1944 onwards the use of wahlworts spread rapidly from the Luftgau keys to Puma and Red until eventually virtually all the Air was infected. The effects in breaking varied greatly according to the strength of the existing cribs on the colour in question, as will be made clear later.

German Use of Wahlworts The usual German practice was to use wahlworts at the beginning and end of each message, i.e. in part messages the wahlworts were at the beginning of the first part and the end of the last part. Occasionally, however, as on the Finches from January 1943 onwards, a more radical method was adopted by which wahlworts were used at the beginning and end of every part. It was fortunate that this extension of the practice was not universally adopted; for (as was keenly realised at the time) it virtually eliminated the popular teil-break technique of solving re-encodements, and this made still harder the already sufficiently difficult African R.E.s.

The length of wahlworts might vary considerably and it was an important part of crib records to note each encoder's favourite length and hence to fix the limits within which cribs should be staggered. As a general rule (though in such a matter general rules are not much good) four to fourteen letters was normal. Rare alike were wahlworts of three letters and the freaks of about forty. Two of the latter deserve to be handed down to the admiration of posterity: the first is the classic:
DONAUDAMPFSCHIFFAHRTGESELLSCHAFTSKAPITAEN, used on a Locust Synoptic and on several occasions on the Finches and the other is the remarkable tongue-twister:
HOTTENTOTTENPOTENTATENTANTENMATTENMAERDER,* which may be translated as "would-be-murderers-of-the-Hottentot-potentates'-aunts." It must be admitted that no other language than German would express the above idea in a single word!

The wahlwort might and often was immediately followed by the text of the message proper; however, some form of punctuation

* This was used on a Gadfly tuning message.

INFO
RESTRICTED

such as X or YY could be inserted. In the last months it became the rule on both Air and Army keys to mark out the wahlwort clearly by doubling the last two letters of the initial wahlwort and the first two letters of the final wahlwort and (assuming no intermediate punctuation) it was possible to use this doubling in making up menus. Thus on Avocet II, which was often broken on GEHEIMEKOMMANDOSAQE staggered to allow for an initial wahlwort, we could if necessary run (??) (??) GEHEIME-KOMMANDOSAQE, secure in the knowledge that each pair of queries would represent the same letter.

Finally, a word must be added on the choice of wahlworts. In theory, this should have been purely random; in practice, it was not. Nouns were almost invariably chosen; individual operators had their favourite wahlworts and some e.g. SOMMER, WINTER, HUNGER occurred again and again. Sometimes also the initial and final wahlworts in a message were connected in sense, e.g. MUSIK....TANZ or in some other way there was an obvious appropriateness. Thus a long part message on Mustard once ended with the "wahlwort", (in this case a misnomer as a phrase was used), GOTT SEI DANK.

But in general such peculiarities were not sufficiently consistent to be predictable and hence usable. There was indeed one instructive exception to this rule. A Mustard operator became so attached to the wahlworts GUTEN....MORGEN, GUTEN....ABEND (each, naturally, at the appropriate time of day) that it was reckoned at one time, viz. in January 1944, that it was better than an even chance that these wahlworts were in fact correct. This was of considerable assistance in reducing the crib versions worth running and on several occasions the initial wahwort GUTEN was used successfully to eke out the otherwise rather brief crib (the Einsatz Mark I).

Effect on Breaking Such an exceptional tour de force, however, cannot outweigh the generally prejudicial effect of wahlworts on our success. It is evident that at best, i.e. when one has good cribs, the introduction of wahlworts may mean the running of three or four versions instead of one; with poor cribs that have several variant forms the case is still worse. Moreover, if there are no real cribs at all one can still do something even with ten-versional addresses if one has to try them in one position only but otherwise the cost is prohibitive. It is for this reason that an address key like Gentian was ruined by wahlworts. As Lincoln might have said, you can run one variant in all positions or all variants in one position; but you can't run all variants in all positions. (Of course, such a statement is false in theory: but it is true in practice as we never had so many bombes that we could ignore the cost in bombe-hours of breaking a key. This meant that for every key there was a limit of costliness beyond which breaks would be made at too extravagant a cost - i.e. at the expense of more valuable colours).

Thus the thorough use of wahlworts will on almost any key make breaking more expensive and on a key with a weak crib position may make it unbreakable except at extravagant cost. This was what eventually happened on the Finches and what would very likely have happened on Avocet in the last months of the war had we not by then in the light of the wahlwort peril and other dangers increased our bombe resources to what would at one time have been considered wildly extravagant excess. It was only owing to this free bombe position that we were able to take the wahlwort strain as well as we did in these last months: and indeed if the Germans had suddenly eliminated wahlworts and started their messages flat

INFO
RECD

again it is possible that like Frankenstein we should have proved unable to satisfy the monsters we had created.

Value of Wahlworts It cannot be denied that in wahlworts the Germans hit on a simple and effective method of making cribbing more difficult. It would have been still more effective but for the eternal German blunder of "too little and too late". Introduced in 1940 on a wholesale scale, wahlworts might have knocked out the infant Crib Room before it had got properly on its feet: but in fact the Germans did not use the system at all till half-way through the war and not until the last few months used it on anything approaching a universal scale.

Yet while a good anti-crib measure the wahlwort is not the best possible prophylactic. It tends to make cribbing harder but not impossible. The rival system (used on Roulette) of burying addresses and signatures in the middle of the message is perhaps preferable though much depends on the nature of the traffic; but best of all such measures is the radical device of the cut. By this any message is arbitarily divided into two parts and the second part encoded first. This simple but effective proceeding should make cribbing quite impossible except perhaps in the case of short messages where the complete text can be guessed. The final judgment on wahlworts must be that the Germans discovered a useful weapon against cribbery but not a complete answer.

1·553 The Mosse Code

The Mosse Code (named after its author, Rudolf Mosse) was invented before the war as a purely commercial code. The code-words were adopted by the G.A.F. and given new meanings. It was used by the Germans on Air keys (never on Army and S.S. keys) from early 1944 onwards, but it was not until 1945 that (in consequence of certain changes in its nature to be described later) it became a factor of some importance as an anti-crib measure. In origin it was probably not intended as such but was meant (like most internal codes in a cipher) to secure brevity in encoding and perhaps to serve as a measure of internal security.

The meanings of some of the codewords were soon discovered from their context; but in September 1944 Hut 3 was able to publish from captured documents the complete code as used in March. It then consisted of approximately 500 five-letter codewords, the vast majority denoting individual units or commands in the German Air Force. Even then, however, a few codewords represented re-current phrases, e.g.

PAPIC = FEHLANZEIGE

and it was this element that was destined to become more pronounced.

In 1945 the code was largely altered and its character changed. It was again possible to build it up from messages and in April 1945 there was published a final revised list of the reconstructed code. It still consisted as always of five-letter codewords but now a far greater number stood for recurrent phrases as opposed to formations of the G.A.F. A few selected examples follow:-

FLYMI = FEHLANZEIGE
GUFWY = VOLLZUGSMELDUNG
JERRO = TAGESABSCHLUSSMELDUNG
JIJUS = ARBEITSMELDUNG
NEPER = EINSATZBEREITSCHAFTSMELDUNG
ORHAF = LUFTLAGEBERICHT

INFO
RECC

and, in addition, dates, times and numbers could be represented by words beginning with T, U, and Z respectively.

It can be readily understood that the replacement of EINSATZBEREITSCHAFTSMELDUNG by NEPER (while technically merely the substitution of one crib for another) is decidedly a change for the worse; for, given reasonable consistency of form, the value of a crib depends on its length. Whether by deliberate intention or not, Mosse certainly discovered a sound security measure. Indeed, the replacement of regularly occurring phrases by brief codewords, (preferably a range of alternative codewords for each phrase) must always be regarded as a useful ancillary to more radical anti-crib precautions. Yet on the other hand some cribs were actually improved by the use of the Mosse Code: this happened when several alternative abbreviations were replaced by the standard codeword.

1.554 Double Encoding

Double Encoding, in contradistinction to the devices already described, was essentially provisional in nature. Its object was apparently by a change in encoding procedure to use without danger a key believed to be compromised but which for some reason could not be immediately replaced. It was a cumbrous procedure and very laborious to the Germans: hence it is not surprising that it was used on only two keys, Raven and Gadfly, and in each case on only a small portion of the traffic. Raven, in fact, only used the device on a single day, March 16, 1944, at least so far as we were aware.

Raven Double Encoding on Raven was made known to us by a fortunate reference in another message on the same day and by an examination of the duds a few doubly encoded messages were found. These messages had to be decoded in two stages. First, one found the message setting in the usual way and decoded the Enigma text: this came out apparently still in Enigma (as indeed it was) but the first twelve letters had the pattern ABC ABC DEF DEF. The next step was to treat ABC DEF as a new preamble, find the message setting and then decode the rest of the message at this setting. The encoding method must be obvious from the above account of the converse process.

Gadfly The method as used on Gadfly was somewhat different. It gave rise to apparent duds but to the credit of Hut 6 the solution was discovered by the Chief Cryptographer before we were told of it by a full explanation in a message. The method is best explained from the encoder's standpoint.

The encoder chose his message setting, say ABC, and enciphered his message in the normal way. Let us assume the message is 234 letters long and he consequently ends at AKC. (We take it that neither wheel 2 nor 4 is in the middle). Then without moving the wheels the operator proceeds to encode in Enigma again the already encoded cipher text.

For the encoder this is simple enough if twice as laborious as usual; for the decoder matters are much more difficult. In the normal way he finds the setting ABC: then he must determine the closing position AKC either by calculation in Hut 6 style or by the German-recommended method, unutterably tedious but fool-proof, of tapping out the message. Having discovered AKC he then decodes the Enigma text to Enigma text and then has to decode this with the original setting ABC truly a case of "Double, double, toil and

INFO
RECC

trouble" if ever there was one!

To complete the subject it need only be said that it is possible with a little ingenuity to run a crib on a doubly encoded message (Gadfly style). Assume, for instance, we have a crib starting TAGESMELDUNG VOM and that the length of the message is 234 as above: then in the simplest case if the doubly encoded Enigma text is PXZPC.....we have a menu starting as follows:-

T ZZA ? ZIA P ZID ? ZZD E

Thus we can build up query menus. These, of course have to be run to allow for all probable turnover assumptions, so the whole process is by no means inexpensive. Yet this method was on several occasions successful in securing breaks.

Summary Double Encoding was used on too small a scale to have any effect worth mentioning on Hut 6 breaking. On the scale on which it was used it must have been no less a nuisance to the German cipher clerks than it was to Hut 6.

INFO

1·56 THE CHANGE FROM WATCH/RESEARCH TO AIR/ARMY

1·560 Introductory

In 1944 the most important change in the organisation of the principal cryptographic sections was the alteration of the whole set-up from a Watch/Research to an Air/Army basis. This change was preceded by a precisely similar alteration on the traffic analysis side by which T.I.S. 1 and T.I.S. 2 were remodelled to deal with Air and Army keys respectively (instead of as previously Watch and Research keys) and it was accompanied by a similar reform in the Registration Rooms. Thus the cryptographic change-over was only one aspect of a profound internal revolution in the whole Hut and while in what follows the cryptographic side only will be considered the influence of the change already made in T.I.S. must not be forgotten. From the administrative standpoint it was so obviously neater and more convenient that one set of traffic analysts should deal with one set of cryptographers that the reorganisation of T.I.S. virtually made inevitable a similar reorganisation of Watch and Research.

1·561 Stages of the Change

The change-over was made in two stages. First at the beginning of October 1944 Air Research was abolished and the whole Air cryptographic effort was amalgamated under one head (Major Manisty): and secondly at the end of November Research (now Army Research only) came to an end and Major Manisty took over the charge of the whole breaking effort. The organisation as it now stood is described in some detail in the next section; the set up before October 1944 can be expressed diagramatically as under:-

HEAD OF HUT 6
(P.S. Milner-Barry)

Watch (Major Manisty)		Research (Major Babbage)	
AIR (Monroe)	ARMY (Nicoll)	AIR (Roseveare)	ARMY (Aitken)

It should be noticed that the internal constitution of the four sub-sections, their personnel and general methods of working remained to a great degree unaltered by the administrative change: the changes that did occur are referred to later. The essential difference between the two set-ups is that the sub-sections were paired together in a new way - this involved changes of locations for some sections - and that in the later set-up there was a definite unity of control (apart from the general co-ordination exercised by the Head of the Hut on all activities).

1·562 Reasons for the Change

These were broadly the same on Air and Army alike. The general contraction of the war into an ever smaller circle round the Third Reich while the Nazis in a terrible fulfilment of Poe's fantasy were being driven relentlessly into the pit of doom made all the fronts more and more mixed up with one another, and this process was inevitably cumulative: it became

harder and harder to justify our neat geographical divisions of Western Front, Eastern Front and so on. Constant liasion was necessary between Watch and Research cryptographers (particularly on the Air side) and it became clear that integration was the only satisfactory answer to our problems. Furthermore, on the Air side the number of keys dealt with by Research had for some time decreased as the Western keys had been transferred to the Watch some months earlier in anticipation of D Day; and if we excluded a few hopeless keys a substantial number of the remainder were in a position to be broken fairly regularly and currently. In short, Research had become to some extent a misnomer and the very success of the section was an argument in favour of its abolition in the old form.

On the Army side the case for the change was not so strong in October 1944 as at that time the Watch and Research Army keys were still on the whole in watertight compartments. Moreover, there were geographical difficulties to be considered; for it was seen that the integration of the Army effort could not be a reality unless the two sub-sections - Army Watch and Army Qwatch - worked in adjacent rooms and this was bound to involve moving the Army Watch (the people engaged in breaking some of the most urgent traffic) further from the operational nerve centre of the Hut - which was the point where Air Watch, Machine Room and Decoding Room converged and there was direct tube and telephonic communication with the bombes. However, the success of the Air fusion made the logical case for the Army fusion irresistible as links now appeared between Army Watch and Research keys- particularly Puffin and the Balkan keys - that were hard to deal with by liasion between two sections working in separate rooms. So the final step was taken at the end of November 1944 and the geographical remoteness of the Army Watch's new quarters was alleviated by the construction of two new conveyor belts, one to bring the decodes to the Army E.P.'er and the other to send them back again without delay on the first stage of their journey to Hut 3.

1·563 Results of the Change

Some difficulties, of course, had been foreseen, chiefly in the sphere of technique; for Watch and Research had developed different methods for dealing with the material presented to them. It was felt, however, that the best elements of the Research technique - careful bulk entering and systematic study of difficult keys and special problems - could be combined with the alertness, speed of action and taking of snap chances necessitated and developed by Watch work. The fusion was successfully accomplished and this was made much easier by the fact that the Qwatch had already developed a technique intermediate between Watch and Research. So the best of Air Research lived on in the Qwatch and the Qwatch Annexe (Room 78), working, however, on more current traffic than had been the case formerly.

On the Army side also the fusion worked well. Quince the Research key most regularly broken, was made a Watch key at once and Avocet was transferred later. In December 1944 the innovation was adopted of blisting (or sorting) all Army keys currently X. This step showed how far the Hut had moved from old conceptions; in earlier days, when it was regarded as essential to blist

X Current dealing with all traffic had been in force on the Air side for some time.

difficult keys with great care when all the traffic was in, to blist everything currently would have been (quite rightly) considered a pure waste of time. The examination of all traffic currently is thus one measure of our general conquest of the Enigma. Yet to the end the Army Qwatch retained much of the old Research atmosphere: this was due to the fact that virtually all the breakable Army keys were transferred to the Watch and only those difficult or impossible to break were left to the Qwatch. This is, of course, just what is apt to happen on the Watch/Qwatch system and everyone understood this: but it happened rather more on the Army than the Air side just because there were so many more breakable Air keys - and of such varying intelligence value - that the Air Watch could not have annexed them all had it desired to do so. And - again because of the greater number of keys - the Air Qwatch worked on Watch keys in a manner that was never necessary on the Army side (see the next section).

1.564 Timing of the Change

It is obvious that the final set-up reached was more logical than its predecessor, and it is also true that the integration of Air and Army effort could in neither case have been longer delayed without harm to our breaking success. But one important question remains - granted that the change was ultimately inevitable and beneficial when made, should it not have been made earlier?

The answer to this question is bound up with the previous organisational changes of Hut 6. It seems quite possible for instance, that had we not made the error previously discussed of separating the Machine Room from the Crib Room we might have reached at an earlier date the final solution of our problems in this direction. But as matters went it was not till February 1943 that the initial error was corrected; and it would certainly have been unwise to complicate the re-organisation then undertaken by attempting to combine it with a change to an Air/Army set-up. It may also be maintained that while it was obvious from 1942 on that in almost every respect there was a great gulf fixed between Air and Army, it was not until discriminants were dropped in November 1943 that it was clear that the Air/Army division was going to be absolutely fundamental for traffic analysis. So on the whole there was no case for effecting the change to an Air/Army set-up before November 1943 and the question becomes whether we should have realised the inevitable trend of events and taken appropriate action between that date and October 1944.

On a difficult question like this opinions may well differ. Logically there was a case for the change at any date after November 1943; but logic is not always a safe guide in matters of administration. From a practical standpoint it is arguable that we were so involved in crisis after crisis in these fateful months that it was the path of true prudence not to complicate the issue by far-reaching measures of reorganisation until a change was clearly indicated. This was at any rate the line followed by the Head of the Hut: and doubtless it coincided with the general conservative sentiment which comes so easily to human nature and which was of very noticeable strength even in so recently formed an institution as Hut 6. Changes were never welcome unless they not only were desirable but were <u>clearly</u> seen to be so.

INFO REC'D

1.565 Unity of Control

The other side of the change effected in October - November 1944 - the unity of control over the whole breaking process - was no doubt also a logical and practical gain. We might, of course, have made this change earlier without any other alteration to our set-up, as is in fact suggested by Mr. Milner-Barry in his introduction. It ought to be mentioned here, however, that in Hut 6 (as in every institution which has grown up from humble beginnings in a natural manner) arrangements that were logically indefensible often worked very well and the dual control of breaking was one of these. The liaison between the personalities concerned was so intimate and close through the daily Lage Conference and other means that the disadvantages one might have anticipated did not in fact arise.

SCRAMBLE
INFO

1·57 THE ORGANISATION OF THE WATCH

1·570 Introduction

The historical development of the Watch and the detailed technical processes involved are fully considerd elsewhere, and this section attempts only to describe the organisation as it was in March/April 1945. Numbers given are approximate, as distribution between the various sub-sections varied as far as possible with the state of work.

The total strength of the Watch was 65, divided broadly as follows:

Air	37
Army	23
Admin. and Signals	5

A more detailed distribution is given in an appendix.

1·571 The Function of the Watch

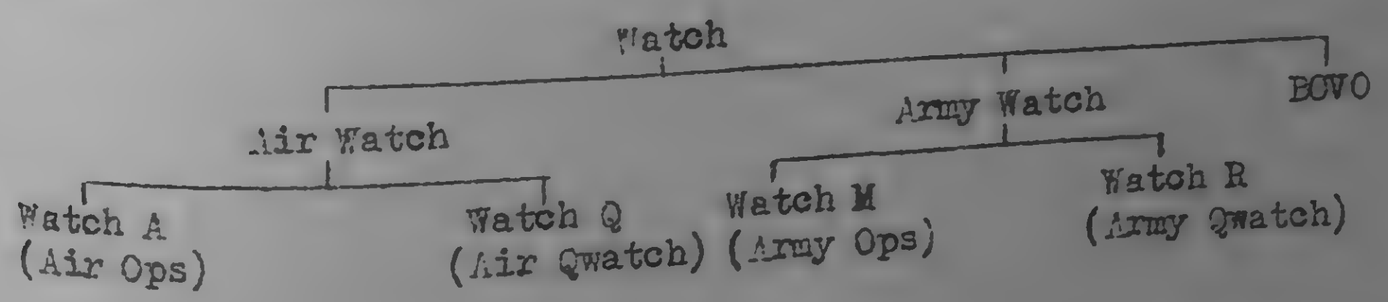
The Watch was sometimes called the cryptographic section of Hut 6. This is a false description, as the whole process of Hut 6 was cryptography and the Watch was responsible for only one stage of this process.

The primary job of the Watch was to examine the traffic already sorted by the traffic analysts and the Registration Room, to find cribs (in the widest sense) on this traffic, to prepare these cribs in a manner suitable for handling by the MachineRoom or for despatch to Washington, to keep the records and do the research necessary to carry out these functions effectively, and to carry out any technical work on the completion of keys that could not be handled by the M.R. The Watch was also responsible for the current running policy on the bombes under the direction of Milner-Barry, acting through the Head of the Watch, and was guided by the machinery described later in the chapter on "Bombe Control". And it was responsible for all signals connected with jobs run in Washington.

A borderline task was menu-making. This was for some time a Watch responsibility, but it had lately become primarily the function of one or two special menu-makers, drawn from the M.R. and sitting in the Watch. The Watch still assisted as necessary, particularly when a number of urgent jobs were prepared at once.

1·572 Basic Organisation

The Watch was divided into two main grouns, Air Watch and Army Watch, and a third small group BCVO whose main function was the handling of signals to and from Washington. The Air Watch and Army Watch were each further subdivided into an operational and non-operational watch (or qwatch = "quiet" watch). The nomenclature may be represented diagramatically thus (the administrative set-up is considered later):-



OFNI 3

The descriptions "Watch A" etc. were never in general use but are used here for precision. In normal usage "The Watch" could mean the whole Watch, the Air Watch, or just Watch A, according to context. This was due to the way in which the organisation grew up and to a certain innate conservatism.

Each member of the Watch belonged to a definite sub-section. Transfers were made as the situation demanded; but transfers between Air Watch and Army Watch were on a long term rather than on a day-to-day basis. Short-term loans were however frequently made from an operational watch to its corresponding qwatch; loans in the reverse direction were rare, as it takes some time for a member of a non-operational watch to become used to operational working.

1.573 Division of Keys between Watches

The division of keys between the Air and Army Watches was simple and rigid - Air keys were handled by the Air Watch, Army and S.S. keys by the Army Watch. But the division between operational and non-operational watches was much less clear-cut, particularly with Air keys.

The basic principle was that if a key was of sufficient operational importance to justify the greater extravagance of current breaking and if there was a reasonable chance of breaking it with some regularity (not of course necessarily every day), then it was handled partially or entirely by an operational watch. Otherwise it was handled entirely by a qwatch.

There were many exceptions to this basic principle, usually in the direction of handling in an operational watch a key which appeared on general principles to be more suitable for complete qwatch treatment. These exceptions arose for two main reasons. It was often more satisfactory to handle together a number of keys in the same theatre which were liable to be connected by re-encodement, even if some of them had no operational urgency. And it was sometimes administratively easier to make a sensible division of work between watches by handling some non-operational keys in operational watches than by transferring members from one watch to another.

Each key had its "parent" or parents, drawn from the watch primarily responsible for it. The amount of special attention given a key by its parents varied from an almost nominal supervision in the case of some operational keys to complete charge in the case of some non-operational keys. The system of parentage has been considered more fully elsewhere.

1.574 Watch A (three shifts)

Watch A was responsible for breaking the operational Air keys; in addition the Head of Shift of Watch A was responsible for the general control of current bombe policy. The latter duty arose mainly for geographical reasons - Watch A adjoined the M.R. - and the Watch H/S was advised by Watch M on the priority of current Army jobs.

The normal shift was five strong, of whom one was designated on the shift-list as H/S. Apart from his responsibility for current bombe policy the H/S was responsible for the distribution of work among his shift and for making sure that the most important tasks were tackled first. He took over from his predecessor a

"lage" (distinct from the more elaborate i/c Ops.' lage) which gave him a summary of the current position on all keys and a note of any special events; he handed over a similar lage to his successor at the end of his shift.

Apart from the finding and preparing of cribs on unbroken keys and the handling of any special machine problems (e.g. breaking a D) there were three routine tasks to be undertaken by a Watch A shift, and each was usually done by a different member. These were:

(a) E.P. Entering - the examination of all decodes en route from the D.R. to Hut 3, and entering of cribs and other worthwhile messages in folders.

(b) Kissing - investigation of the potential re-encodements thrown up by the sheets of kiss-pairings prepared by the R.R.

(c) W.L.P. (Watch Liaison Party) - two-way liaison with Control, I.C.I., and other sources of information on matters of cover and identification. This task was a recent addition caused by the new callsign and frequency system.

None of these tasks was necessarily full-time and it was usually possible for the member concerned to assist in the finding of cribs. The H/S distributed these three tasks and the handling of the various unbroken keys to the members of his shift. He took a share of the work himself, but was wise to leave himself sufficient free time to keep general control of the proceedings. An unbroken key of first importance might well be looked at by more than one person, and by tradition anyone was at liberty to look at a key which had not been allotted to him without any feeling of"poaching".

In addition to the five Watch members of the shift there were also in the same room two or three members of the M.R., working under the general guidance of the Watch A H/S. These were the i/c Ops., who handled the bombing of individual jobs and kept the necessary lages, and one or two menu-makers.

In addition to manning the three routine shifts, three members of Watch A were usually working in Watch Q, and it was often possible for other members to have a few days off shift in order to deal with particular problems or to give special attention to the keys of which they were parents; otherwise parental duties had to be carried out during slack time on a routine shift or in spare time.

1.575 Watch Q

Watch Q is certainly the most complicated sub-section to describe; the simplest method is probably to split it up into its component parts and to give the primary functions of each of these parts. The distinctions were not at all rigid - the great merit of Watch Q was its flexibility and ability to turn its quite considerable strength wherever required.

Watch Q worked in two rooms - Room 64 adjoining Watch A and Room 78, which was not far away but quite distinct.

Room 64

Head of Watch Q (Taunt). Responsible for the work of Watch Q as a whole and particularly for co-ordinating all activities in

Room 64, and keeping in touch with heads of shift of Watch A.

Kiss Clearance (two strong - two shifts). Responsible for checking kiss-lages dealt with by Watch A, for investigating any re-encodements not fully dealt with by Watch A, and for checking and investigating re-encodement information supplied by Sixta.

Q.E.P. (five strong - three shifts). Originally started when thrice-daily stecker was threatened as a "Qwatch Entering Party" to maintain fuller records of keys than could be done by the regular entering system. This was still their primary responsibility on keys on which it was found necessary, and the party was available for any special entering projects. But the members trained in other jobs and two at least of them had become very useful general hands. Q.E.P. night shift handled the Washington signals, a job performed by BOVO on the other two shifts.

Watch A Party (three strong - two shifts). This party which included a H/S from Watch A, worked in co-operation with Taunt on recalcitrant Watch A keys which needed more sustained treatment than could be given on normal shifts.

Room 78 (five strong - one shift). In charge of Roseveare, who also acted as deputy to Taunt. Responsible for most keys not handled by Watch A (a few were sometimes handled in Room 64 when state of work permitted) - notably Eastern Front keys at the end. This was the only really non-operational part of the Air Watch.

1.576 Watch M (three shifts) and Watch R (one shift)

Watch M was responsible for breaking the operational Army keys and worked with a shift of four, of whom one was designated as H/S. The responsibility of a Watch M shift was similar to that of a Watch A shift with the exception of control of bombe policy; however, the H/S in Watch M advised on the priority of current Army jobs. There was in Watch M no special job of "W.L.P.", but any necessary liaison was normally carried out by the H/S.

The division of work between Watch M and Watch R was much more rigid than that between Watch A and Watch Q. Something analogous to "Q.E.P." and to the "Watch A party" in Watch Q did however exist, but was considered part of Watch M. One member of Watch M, working normally on day shift, was particularly responsible for keeping records, but often had time to assist with the current work of the day shift. And one member, usually of H/S status, was designated on the shift-list to work "non-routine"; he had no responsibility for current breaking, but concentrated on recalcitrant keys and any problems on Watch M keys that needed research.

Watch R was entirely responsible for the Army and S.S. keys not handled in Watch M. The regular members of Watch R were supported by one visitor from Watch M on a weekly changing basis. And there was in Watch R one specialist enterer analogous to Q.E.P.

1.577 BOVO (two shifts)

The first responsibility of BOVO was the handling of signals concerning Hut 6 jobs in America and the maintenance of all necessary records. On the night shift a member of Q.E.P. handled the signals; it was not a full-time job on this shift and the Q.E.P. member was able to devote part of the time to her normal duties. BOVO worked directly under Manisty, who was responsible

USAF
INFO

for general relations with Washington, and it also assisted him in administrative and secretarial duties.

1.578 Administration

The only purely administrative member of the Watch was its Head, (Manisty), who had found it necessary for the last year to keep himself clear of other work. Apart from general responsibility for the policy and organisation of the section, he controlled the arrangement of shifts and leave for the whole section; this was thought more satisfactory than dividing the responsibility up among the sub-sections, as considerable co-ordination between the various shift-lists was necessary. Semi-technical points of administration - for example, the control of special cover on crib frequencies - were delegated to members of the watches concerned.

Monroe was Manisty's deputy; he worked normally in Watch A of which he was the senior H/S, but was detached from normal Watch A work when Manisty was away. Each of the four watches had in effect a recognised head and deputy-head; the technical organisation of A and Q was more directly under the central control than that of M and R.

Two criticisms can be fairly levelled at this as a theoretical organisation. The first is that there was no definite head of the Air Watch (A and Q) (except Monroe in his capacity as deputy head of the whole Watch) and no definite head of the Army Watch (M and R). The second is that the Head of the Watch had no administrative assistant at a high enough level to take responsibility, and so was perhaps too much involved in administration and did not see enough of the actual work of the rooms. These defects were largely due to the way in which the section was formed and to the personalities involved. But they were also due to a reluctance to detach a competent technician from his technical work and "waste" him as an administrator - whenever we considered doing it, we thought: "It is a bad moment just now, but perhaps in a few weeks' time....."

SCAN INFO

1.579 Appendix: Detailed Distribution of Members

	Manisty	1	1
Watch A	Monroe, H.F.T. Smith	2	
	Others normally acting as H/S	4	
	Occasionally acting as H/S	2	
	Other members	15	24
Watch Q	Taunt	1	
	Kiss clearance	2	
	O.E.P.	5	
	Roseveare	1	
	Room 78	4	13
Watch M	Nicoll, Read	2	
	Others normally acting as H/S	4	
	Enterer	1	
	Other members	11	18
Watch R	Aitken, Gaunt	2	
	Enterer	1	
	Other members	2	5
BOVO	Members	4	4
			65

Men	British	23
	U.S.	11
Women		31
		65

SECRET
UNCLASSIFIED

1·58 FINAL DEVELOPMENTS OF THE RULES OF KEYS

1·580 Introduction

In the last period of the war from January 1944 to May 1945 there were a number of interesting developments in the sphere of key rules but most of them were simply extensions and applications of rules already known. There were no radically new discoveries comparable in importance, for instance, to that of the Nigelian wheelorders. Hence it will be possible to deal with the subject more summarily than in previous periods and an endeavour will be made to avoid the extreme detail which is inevitable in current reports but is confusing in a bird's-eye view. It is accordingly proposed to select from the reports of the Committee on Rules of Keys only the more important tendencies and the more interesting special details. It seems best to consider in order the regular Air keys, then a few special Air keys, then the Army keys with a final note on the rules of D.

1·581 The Regular Air Keys

(1) Wheelorders The Nigelian rule maintained its sway till the end unchallenged by any rival; though at times anarchic tendencies appeared to be gaining ground and there were many non-Nigelian keys. What was more serious, in some months an alarming number of breaches of the fundamental non-clashing rule occurred. Such lapses were the more unfortunate as now wheelorder rules were the most practically useful of all key rules: the days of hand breaks were past, but any rule that saved bombe time never lost its value. However, the growing disregard of wheelorder rules that was marked from spring to autumn 1944 was at last checked and by December it was possible to say that there was a distinct improvement which mercifully continued till the end of the war.

(2) Ringstellung At first ringstellung rules appeared not infrequently, though owing to the decline of cillying we were hardly ever able to turn them to practical account. Apart from the old 26-day rule, several new varieties appeared. For instance, in December 1943 and January 1944 several keys had no repeats of ringstellung letters in the last 26 days of the month i.e. from the 6th to the 31st. More original was a new rule first seen in March 1944 on Puma and Primrose by which the letters of the alphabet plus one repeat formed a block of nine consecutive days. (There was considerable variation in the days that formed the block: in October 1944 when this rule was popular we find several keys that "block" 30-22, 21-13, 12-4, another that prefers 31-23, 22-14, 13-5 and another that takes the simple course 1-9, 10-18, 19-27.) It will be noticed that this rule is more akin to the Army ringstellung rule than any previous Air rule; yet towards the end of the war (from January 1945 on) it was the only ringstellung rule observed by any Air key and even this rule was observed by very few. But the influence of ringstellung rules on our breaking had for long been so negligible that few even noticed their disappearance.

(3) Stecker So far as regards rules in the strict sense, nothing was added to what was already known -- viz. the avoidance of consecutive stecker pairings and the tendency to diagonalisation. However, from the Parkerian records a number of stecker repeats were discovered -- far fewer than in the palmy days of 1942-3, but none the less not to be despised.

The first of these was a batted stecker repeat between two of

our less important keys -- Leek and Celery of April -- which despite its irregular nature and its occasional inexactitude was successfully used on several occasions towards the end of the month. Later there was a new batch of stecker repeats which are listed below, some of very short duration which ended almost as soon as they were discovered and others from 1944 to 1945 -- this last was an innovation, as no previous key repeats of any kind had crossed the turn of the year.

The particular stecker repeats were as under:-

(a) Cockroach 5,6,8,4/10 = Cricket 20, 22, 25, 26/10
(b) Daffodil 4,5,1,2,3/11 = Lily 22, 23, 27, 28, 29/11
(c) Red November = Red December (hatted repeat)
(d) Ermine 15-31/12/44 = Jaguar 1-17/1/45
(e) Cockroach 1-30/11 = Beetle 20-31/12, 1-3/12, 5-19/12

It is worth mentioning that by no means all these repeats were exact: in some cases as many as three stecker pairings were altered. Our system of recording sets of stecker and looking for repeats did not inevitably pick up such slightly altered repeats; and the whole matter was discussed with a view to devising a more certain method of picking up useful repeats, probably by the use of Freeborn machinery. However, before much was actually done on these lines, the partial repeats had come to an end. In fact, the only remaining stecker repeat discovered was a hatted one between certain days of February Hyena and February Daffodil.

1·582 Brown, Yak and Llama

These special keys went their own way. Yak and Llama were locally issued Fliegerführer keys which did not observe the central Cipher Office rules of Nigelian and non-clashing wheelorders and avoidance of consecutive stecker. Yak in addition had on occasion the peculiarity of repeating its own keys. Thus in January 1944 Yak repeated the keys of December 1943 in a chopped and jumbled manner: it was possible to some extent to predict wheelorder and ringstellung, but the sets of stecker were completely hatted. Something similar occurred in November 1944. For the first fifteen days of the month Yak repeated the stecker of the first fifteen days of September, not day for day but in little runs of two to five. Except on November 14 and 15, the wheelorders and ringstellung were different permutations of the corresponding September day's key. For the last fifteen days of November the stecker repeated stecker of the last half of October in little runs, without any repeat of wheelorder and ringstellung.

Llama's peculiarity was the use of an unusual number of self-stecker, like Brown. When it was first broken in January 1944, the limits varied from 10 to 16 self-steckered letters. In April, however, seven stecker pairings became the rule with I and L always self-steckered. In May and June there was more variation, but always a large number of self-stecker; finally, however, in July the normal ten stecker came into force.

Brown by now, it will be remembered, had also the normal ten stecker and so the characteristic stecker pairing rule was impossible However, to compensate for their refusal to adopt the regular Air rules Brown I and III invented some of their own. Brown I indulged in a key repeat. February 15-March 14, 1945 repeated the keys of August 15-September 14, 1944, but, unfortunately for us, not day for day. Each February-March day had the stecker of some August-September day and the wheelorder and ringstellung of the same day,

OCR INFO

possibly permuted and not necessarily in the same way. (This meant that for each set of stecker available there were 36 possible keys.) It can easily be imagined that this kind of repeat was not easy to exploit, and after the resources of rodding had been exhausted we were reduced to a massive decoding assault in an unfortunately unsuccessful attempt to clear up the five or six missing days.

On Brown III a useful stecker/wheelorder rule had a reasonably long run. From October 15, 1943 to March 14, 1944 -- i.e. five consecutive Brown months -- only 30 sets of self-stecker were used and each was associated with one or two (in one case with three) wheelorders; a permutation of an associated wheelorder was always used with each set. This rule was successfully utilised in breaking several days. Later, from April 15 to May 14, Brown III repeated day for day the sets of self-stecker used in February-March.

Brown III was also involved in the last key repeat ever discovered -- Brown III of March 1945 repeated the keys of February Cockroach. This repeat seemed to imply that at long last Brown had forfeited its independence and that the G.A.F. Cipher Office had gained control over its keys: it is, however not quite certain that this is the true explanation. It may be that the Brown keymaker had somehow got possession of the Cockroach key and with characteristic disregard of cipher security decided simply to use it again.

1·583 Army Keys

(1) Wheelorders From a general point of view there is little to report in this line except that as time went on clashing wheelorders became rarer until in March 1945 it became reasonable to give a preference for the 32 non-clashing wheelorders on nearly all Army keys. There were, however, a few oddities. One such was that the Railway key, Culverin, only used wheels 1,2 and 3 like Tricycle of old. Another peculiarity was found on Ibis of December. Out of 15 days broken 14 had a 3 in the wheelorder, clearly not a fortuitous occurrence. There were also a number of wheelorder repeats viz. days 1 and 12; 5 and 15; 7 and 19; 8, 20 and 30. This suggested that the compiler of the key had split the month into three sections and used roughly the same wheelorders in each period, but we were unable to test this hypothesis further. In no other month did Ibis show any comparable peculiarity.

(2) Ringstellung The old Army ringstellung rule was not seen after January 1944 and no new rule took its place. The increase in stuttering ringstellung has been noted elsewhere. Apart from this, we have only to note a few oddities -- for instance, from February to April Wagtail, the practice key of Wehrkreis VIII, had a ringstellung which only differed from that of Falcon I by being two less on the first wheel. (The rest of the key was the same as Falcon.) Again in July 1944 Nightjar repeated its ringstellung in a peculiar way. Days 11-19 repeated the ringstellung of 1, 3-10 (with an alteration of a letter in a few cases) and most of the days 20-31 had for ringstellung some permutation of a ringstellung previously used.

(3) Stecker Here we have to record a few cases of partial repeats within the same month and also a new form of stecker pattern. The partial repeats occurred on Nightjar of July 1944 (already mentioned under ringstellung) and Falcon I of January 1945. On Nightjar there was a repeat of sets of self-stecker at irregular intervals -- out of 29 days broken only 14 self-stecker sets were used, some as often as three times e.g.

SECRET INFO

C E F H K M 1, 16, 28 .

I K M N P X 4, 11, 31

As can be readily conjectured, it was impossible to use such an irregular repeat.

Falcon of January 1945 had a more predictable and hence more useful self-stecker repeat. The days fell as a rule into blocks of from 2 to 4, each block having throughout the same self-stecker. or only slight variations. Thus days 4 and 5 had self-stecker D G H J V Y and days 6 to 9 A L M S W X while days 1 and 2 had I N Q W X Y and day 3 I N Q R W X. In two cases at the moment of transition from one block to the next the self-steckered letters of the first block were paired together for the first day of the next block.

The stecker pattern was found on Orange of August 1944 up to the 20th when it suddenly ceased. The days were divided into consecutive pairs with the same set of self-stecker and the stecker so altered that, for instance, A/L D/O on the 1st became A/O D/L on the 2nd. It was unfortunately impossible to make use of this transposition of stecker, as we had no means of telling which pair of stecker were to be transposed: this was doubtless determined by the arbitrary order on the German key-sheets. However, the knowledge of the six self-stecker was very useful in making more easily runnable the short Orange cribs.

(4) Repeats In this last period of the war there were rather more Army repeats than previously. The Wagtail/Falcon repeat has been already mentioned but in addition there was a new feature -- repeats on S.S. keys. Quince of March repeated Orange of January, wheelorder and stecker being repeated in reverse order, ringstellung in the same order. (In the Quince key a few ringstellung were slightly altered to avoid stutterers.) This repeat was of inestimable cryptographic value in enabling us at a critical period in the history of the key to break and decode a whole month's Orange traffic. About the same time E/320, a practice key which only passed the German High Command communiqué and had no intelligence value, was found to be using elements of S.S. keys -- to judge from the only two breaks obtained in January 1944, this key was indulging in a hatted repeat of ringstellung and stecker from January Quince. Like most hatted repeats, this was of very little use and could not be exploited.

A key repeat of an original nature, charming in its naiveté, was provided by Penguin, a home-made divisional key of the 12th S.S.Pz. Division. From its first appearance in June 1944 Penguin only used six keys, two of which were very similar, only differing by a slight change in the ringstellung and a permutation of the wheelorder. The six keys were used in regular sequence, the cycle starting anew on the 1st of every month. It did not take us long to break all six keys and thereafter Penguin was out automatically as long as it lasted.

1·584 Rules of D's

It was discovered by August 1944 and confirmed by all subsequent breaks that consecutive pairings were avoided in Air D's -- of course, for the present purpose German notation is assumed. This is in line with the avoidance of consecutive stecker pairings: to the Germans there was no difference, as they styled D pairings

SECRET
INFO
3

stecker pairings in the reflector. The Army, as might have been expected, had no such inhibition and the D for NOT-keys (see the section on Notschlüssel) was wholly alphabetical -- i.e.
A/B C/D E/F G/H I/K L/M N/O P/Q R/S T/U V/W X/Z

The number of D's used per month was originally three, but after some fluctuation in October 1944 settled down to four in November.

In all other respects the keymaker had a free hand in constructing D's except that he had to write down only 12 pairings, omitting the letters J and Y which corresponded to the permanently fixed D pairing (BO in our terminology). The curious repeat between D wirings and stecker sets has been dealt with in a previous section.

1·585 Summary

The study of key rules never justified the more ambitious hopes of its pursuers: it was never possible, except for brief intervals on Brown I, to reduce everything to rule and write down a key from its predecessor. From the sporting point of view this was just as well: the discovery of a complete German system of keymaking, however gratifying in other respects, would have meant the end of Enigma cryptography in any real sense.

Yet it cannot be denied that the study of key rules and the associated search for key repeats paid immense dividends, particularly in 1942. On a mere basis of statistics hundreds of keys must have broken by this alone; and what is more important we made our first entry by this means into many keys that otherwise we would never have broken or at least much later. The experience in Hut 6 shows clearly the necessity in similar circumstances of examining all keys carefully and keeping thorough records. One must never argue that the enemy cannot be so stupid as to have key rules or repeat keys he has already used. If to underestimate one's enemy is a sure road to disaster, to overestimate his cleverness may result in overlooking that he has made the most obvious mistakes.

CHAPTER 1.6

B O M B E C O N T R O L

1.60 INTRODUCTION

No attempt is made to describe the growth of the bombe control problem and the various measures taken from time to time to deal with it. Some mention of these will be found in I.J.Bellis-Bonny's General Introduction. All that is done here is to state the problem as it existed in May 1945 and to describe the machinery that had been set up to handle it.

Largely on account of the way in which the sections grew up, Hut 6 and Hut 8 maintained independent machinery for bombe control; there was necessarily close contact between the two Huts, as a large proportion of the bombe strength was usable by either. The problem is considered here from the Hut 6 standpoint - the large number of different keys made it a much more complicated problem for Hut 6 than for Hut 8.

There are two aspects of the problem which although connected can be considered separately. They are the policy aspect and the operational aspect. The former includes the distribution of the bombe strength between Hut 6 and Hut 8 and between the various Hut 6 keys; the latter the actual minute-to-minute handling of individual jobs.

1.61 THE PROBLEM

At the beginning of May 1945 the following bombe strength was available in England and America:-

England	14	4-wheel bombes usable only by Hut 8.
	42	4-wheel bombes usable by Hut 8, or by Hut 6 for delayed hoppity jobs.
	12	4-wheel bombes usable by Hut 8, or by Hut 6 for ordinary jobs.
	50	3-wheel bombes usable by Hut 6 for ordinary jobs or by Hut 8 on their only remaining 3-wheel key (Bounce).
	89	3-wheel bombes usable by Hut 6 only
America (Op-20-G)	112	4-wheel bombes usable by Hut 6, or by Hut 6 for delayed hoppity jobs.
(Arlington)	1	144-enigma 3-wheel bombe, usable only by Hut 6 and equivalent to four ordinary bombes.

1.62 "INTELLIGENCE VALUE"

The sole object of cryptography is to provide intelligence. Before considering the policy aspect of the bombe control problem it is therefore worth discussing briefly what is meant by the "intelligence value" of a break.

At its simplest the intelligence value of a break means the amount of intelligence that is obtained from the decodes of traffic on the

broken only. But this is an inadequate criterion of the real intelligence value of any given break. For example, with certain types of intelligence continuity of information greatly increases its value. A break of such a key does not only have intelligence value in itself but also increases the value of breaks of neighbouring days. Again distinction is sometimes made between the "intelligence value" and the "cryptographic value" of a break; this distinction is false. What is meant by saying that a break has cryptographic value is that it assists in some way - for example, by re-establishment on key aspect - in the breaking of further keys and hence in the provision of further intelligence. Thus the value of such a break is not merely judged by the intelligence provided by the decodes on the key itself.

It is in this wide sense that the expression "intelligence value" is used when considering bombe policy. But even then it is not purely quantitative. There is a distinction between "urgency" and "importance", although these two qualities cannot be completely separate. A different policy can be adopted with a key whose breaking will immediately affect current operations and a key whose breaking is important for planning but will call for no immediate action. And certain keys of little importance such as weather keys may not be worth breaking at all if they cannot be broken currently.

1.63 HUT 6 - HUT 8

All sections concerned in Bletchley Park accepted and worked on the principle that the bombes should be regarded as a general pool and that the potential intelligence value(used in its widest sense) of the keys concerned combined with the expenditure of bombe time necessary and the chance of breaking should determine priority.

The position in America was not quite so straightforward. The Op-20-G(Naval)bombes,which formed the greater part of the American bombe strength, had been built specifically for naval problems, in particular for Shark. But in practice this did not cause great difficulty, and apart from the overriding priority of Shark,Op-20-G effectively accepted the pool principle and their bombes had become a major factor in the breaking of Hut 6 keys.

In order that the relative value of Hut 6 and Hut 8 keys could be discussed and general working principles laid down there were regular weekly meetings between the parties concerned; such meetings took place in Hut 8 and were attended by representatives from:-

Hut 6
Hut 8
Hut 3 (3 M)
Naval Section
Op-20-G

At these meetings a general line of policy was agreed, and it was left to the Hut 6 and Hut 8 representatives to issue the necessary administrative instructions. Op-20-G were also informed of any changes of priority. If a new situation suddenly arose an emergency meeting was called.

1.64 HUT 6 KEYS

1.641 Responsibility

The Head of Hut 6 was finally responsible for bombe policy, but its current direction was delegated to the Watch and was the immediate responsibility of the Air Watch head of shift. He negotiated with Hut 8 regarding allocation of bombes between the two Huts on the basis of the decisions of the weekly meeting. At one time these negotiations could be rather complicated, but recently they presented much less difficulty, as all Hut 8 keys except Bounce were 4-wheel, and only 42 bombes were therefore concerned unless Bounce was to be run.

To assist the Watch in deciding the relative priority of various Hut 6 jobs two routines had been instituted - a daily meeting with 3 L (the liaison section of Hut 3), and a complete list of Hut 6 keys arranged according to intelligence priority.

1.642 Daily Meeting

This meeting served not only as a guide for the Watch in its current work but also as an opportunity for a general exchange of information. It was normally attended by Milner-Barry, Manisty, the heads of shift from the Air and Army Watches, representatives from the Air and Army Qwatches, and a representative from 3 L. A"lage" of non-current(more than one day old) jobs was typed and served as rather arbitrary agenda for the meeting. The four Watch representatives gave brief accounts of the situation and answered any questions. The 3 L representative mentioned any points of special intelligence interest. The Watch representatives could then withdraw, and the three remaining at the meeting graded the non-current lags - i.e. put the jobs into an order of running, which was passed on to i/c Ops.

This last procedure may sound rather illogical, as jobs run at Washington rarely came under discussion at all. The meeting was instituted at a time when there was a strong distinction between Watch and Research keys and when bombe time was heavily in demand, largely in order to ensure that the most important jobs on Research keys were given priority, if necessary over the less important Watch keys. At that time the Washington bombes were not a significant factor. But even at the end, when there was rarely much delay in running any jobs produced, the existence of the lags perhaps prevented the meeting from degenerating into vagueness by giving it actual decisions to make. Certainly Milner-Barry, Manisty and 3 L found the meeting of real use as a means of keeping themselves in touch, but the Watch representatives sometimes regarded it with some impatience.

1.643 Priority List

For the last year of the war a list of keys arranged according to intelligence priority was issued regularly on information supplied by 3 L. In its final form the list contained all Hut 6 keys being broken or likely to be broken. The keys were arranged in 6 classes for importance and in 6 classes for urgency. It provided a very useful guide to the Watch(and to other rooms) in deciding priority of current work, and also gave a convenient classification of Hut 6 keys when the relative claims of Hut 6 and Hut 8 were under consideration - Hut 8 keys were sufficiently few in number to be

considered individually in discussions.

1.65 CURRENT BOMBE CONTROL

1.651 England

Three members of Hut 6 were directly concerned with current bombe control:

In Watch A (Operational Air Watch)	The H/S i/c Ops (a member of the M.R. working in the Watch for a particular shift)
In the Machine Room	O.C.B. (i.e. O.C.Bombenlage)

O.C.B. was in direct touch with the Controller in Hut 23, and was concerned with the placing of every bombe (except those in use by Hut 8); when a bombe finished a job, she would tell the Controller what its next job was.

I/c Ops kept a complete current record ("Lage") of jobs running and available. This lage was arranged under keys (O.C.B., however, was fundamentally concerned with bombes) and was divided for convenience into Air and Army, each being subdivided into current and non-current. ("Current" was arbitrarily taken as "not more than one day old"). I/C Ops advised O.C.B. of the order in which jobs should be run, but was not concerned with the placing of individual bombes except where jobs demanded bombes of a special type.

H/S in Watch A was responsible for the general policy being carried out by i/c Ops. He could see the current position from the lage and advised i/c Ops of the order in which she should run current jobs and on such points as whether to run more than one job at a time on the same key. The order of running non-current jobs had been decided at the meeting, but H/S was responsible for fitting in jobs produced after the meeting.

The lage was rewritten by i/c Ops at the end of her shift, and the old lage passed to the section of the Watch concerned for checking its records.

The detailed technique of bombe control in the Machine Room is considered in the following chapter, but two aspects of the problem are closely connected with policy and are worth discussing here.

The first is the problem of how many bombes to put on a given job. The most economical method is to put one bombe on to each menu and turn to avoid unnecessary plugging. This in fact was rarely done even with non-urgent jobs unless a few wheelorders only had to be run. With urgent jobs one bombe per menu is too slow and with non-urgent jobs it makes for inflexibility. Now the situation frequently arose of an urgent job being produced at short notice. If this was a job requiring a large number of bombes, e.g. a crib of which several versions had to be run, or a naval job to be run on some 300 wheelorders, the only way to obtain the bombes quickly was to remove some from non-urgent jobs. If these jobs had at least two bombes per menu, it was usually possible to obtain enough bombes for the urgent job and still to leave at least one on each of the non-urgent menus. It was

then unnecessary to strip the non-urgent job completely and to replug it at a later stage, with advantage both to the administration of the bombes and to the morale of the bombe operators;with the number of bombes in use and pressure on communications administrative convenience in running bombes was really important. In fact the normal routine was to put two or three bombes on any menu running 60 wheelorders.

The second is the problem of the use of special bombes,in particular those English bombes that can run delayed hoppity menus which otherwise have to be sent to Washington. To run an urgent job in a reasonable time it is necessary to put at least eight of these bombes on to a 60-wheelorder menu. And, as these bombes were also in demand by Hut 8, their control was rather more a direct concern of the H/S than the control of the ordinary bombes.

1.652 Washington(Op-20-G)

The ideal would have been to apply to the control of the bombes at Washington exactly the same methods as were used here - in fact to use them as part of the general stock. But communication difficulties made this impossible, and a much less flexible system had to be used. By means of a system of priority indications we were able to use these bombes fully operationally, although the most urgent jobs were when possible run here. But the bombe strength available for delayed hoppity menus at Op-20-G was much greater than that available here, and so with the growth of the use of short cribs we made considerable use of Op-20-G for jobs of the first urgency. And certainly for these jobs they gave very good service indeed, delays being solely due to the inevitable difficulties of communication.

A standard form of signal was used for sending jobs, and these signals were encoded by the Cipher Office on the C.C.M. Signals all went through Hut 8 but were prepared in Hut 6 by a small sub-section of the Watch, known as BOVO. (BOVRIL and OXO were cover names for jobs at Op-20-G and Arlington respectively). BOVO kept all records connected with jobs at Washington, and prepared twice daily a statement of the jobs in hand at Op-20-G together with the fate of jobs that had been run since the last report. The morning statement was circulated to all concerned, including Milner-Barry and 3 L, and so gave those interested an opportunity of suggesting alterations of priority.

There were five classes - D, DE, E, F, G; D was strictly confined to jobs of high urgency and Op-20-G treated D jobs on a level with the most urgent Hut 8 jobs. G was rarely used. It was unusual for more D and DE jobs to be sent than could be handled at one time, and so normally they were given no special priority among themselves. If pressure was heavy,a special note about priority was made in the job signal. Within each class a serial number was allotted to each job, and in classes E, F, G the relative priority was determined by the serial number, the lowest number being run first, and decimal subdivisions used where necessary.(For example, F 45.1 was run before F 46 but after all E jobs). Jobs were graded and numbered by Menisty(or deputy)when on duty, and at other times by the H/S in Watch A or Watch M.

Op-20-G sent us three times a day a statement of jobs running and jobs completed since the previous statement. In addition, if a job came up there, a clear signal was sent under the code word"AUDIT"

referring to the time of origin of the job signal; this gave advance information that the job was up and enabled work on the key to be stopped here - the key itself followed in a cipher signal about an hour later. A similar procedure was used to indicate that D and DC jobs had gone down, but was not found necessary for lower priority jobs.

1.653 Washington(Arlington)

The method of control of the Arlington bombe was similar to that used with Op-20-G. Signals were prepared by BOVO; they did not pass through Hut 8, but were sent direct to the Signals Registry by tube. The priority categories here were A, AB, B, C and it was not normally found necessary to indicate priority with a class. The much smaller capacity of the Arlington bombe made the control problem simple, and only at times of high pressure was it used for urgent jobs. The only exception to this was the rare occurrence of an urgent cilli job in two or three periods - such a job could only be run by the Arlington bombe.

1.66 CONCLUSION

The inconsistencies in this system of Bombe Control - as in many other Hut 6 routines - were largely due to the way in which it grew up. On the whole it worked, although starting from scratch something rather different would probably be designed. In particular the maintenance by Hut 6 and Hut 8 of independent control systems inevitably caused some loss in flexibility. But this was a consequence of the existence of the two Huts as separate units, which arose for reasons of history rather than of deliberate planning.

CHAPTER 1.7

HISTORY OF THE MACHINE ROOM

(FORMERLY NETZ ROOM)

1.70 HISTORICAL OUTLINE

Throughout every change the general function of the Machine Room (originally the Netz Room) in Hut 6 remained the same. It was throughout an ancillary cryptographic section, assisting at every stage the principal cryptographic sections --first Machine Room and Crib Room, later Watch and Research --in whatever way was most suitable at the time. In the last years this assistance was given primarily in the field of bombe control and testing of stops and for this reason the present chapter follows on naturally from the last.

Historically the development of the Machine Room falls roughly into three parts:-

(1) The original Netz Room, occupied first of all in the preparation of the Netz sheets and then for the first half of 1940 in the shoving of the sheets to break keys. This work was highly important and demanded the greatest concentration. In the latter half of 1940 with the change in indicating system this work disappeared and the members of the N.R. were usefully (but perhaps somewhat monotonously) occupied in performing various odd jobs for other Rooms -- e.g. sticking decoded tapes on messages for the Decoding Room, or punching Banbury sheets for the Research cryptographers in attempts to break Greenshank.

(2) The interim period, when the Netz Room took over from the Machine Room (but still under their supervision) the work of testing bombe stops and later finding ringstellung. The name Netz Room, though now a misnomer, was still retainedfor traditional and sentimental reasons.

(3) The final period, after the Machine Room and the Crib Room had been combined and renamed the Watch. The Netz Room then took over completely the duties of direct bombe control and testing, and themselves became known as the Machine Room, a logical but at first rather confusing, step.

This report dealsalmost wholly with this last stage of development i.e. from 1943 to the end of the war. It should be mentioned that from April 1942 while technically the N.R./M.R. worked closely with the cryptographic sections, administratively it was placed (along with both Registration Rooms and the Decoding Room) under the charge of Mr. Fletcher.

1.71 EXPANSION OF THE ROOM

During the last years the Machine Room was continually expanding and adopting new methods of organisation to meet the demands of the rapidly increasing number of bombes. It says much for the ability and personality of Mary Wilson, the head of the room, that all the improvements and changes were carried through so smoothly and efficiently.

Some idea of the vast increase in the volume of work is given by the fact that in 1942 a shift of 6 or 7 was able to cope with the work of allotting the bombes, testing stops, finding ringstellung, registering and breaking Rocket and attempting to break dud messages. (The last two jobs were always regarded as subsidiary functions of the M.R. and eventually they were delegated to a separate sub-section; more will be said of duds later, while

a report on the breaking of Rocket will be found attached to the history of [illegible]'s Section.) In 1945 a minimum of 13 was needed, and by this time Rocket and Duds had been transferred, the number of sheets per menu had been greatly reduced by various means to an [illegible] level, and a great deal of operational work connected with bombe-running (e.g. the checking of wheel-orders) had been transferred to Hut 25, the central bombe station situated [illegible], and the subsidiary outstations. At least half the women of the shift were engaged in organisation, and were kept busier than one girl had been in 1942, doing the work of all of them. The M.R. was the last Room to adopt the system of heads of shift, but this became necessary when the shifts became larger, and the division of work more complicated.

The third big expansion came in October 1942, when the first influx from the Universities arrived, and, by the time the move to Block D took place in February 1943, the rooms in Hut 6 were very overcrowded. At first the new quarters seemed luxuriously spacious. Three rooms were alloted to the M.R., one for testing stops etc., one for Pocket and one for Duds. Unfortunately, by the time these rooms would have been well-filled they were taken away -- first the Duds Room for the Decoding Room School, and later the Rocket Room for an extension to the D.R. Room 1 in Block D was then used for Rocket, but the main testing room became very crowded, and remained so until the end.

1.72 THE BREAKING OF DUDS

Before discussing the final set-up for bombe control, it seems best to deal with this minor function of the M.R. By the end of the war it had mainly been delegated to a separate sub-section, presided over by the indefatigable Miss Epperson, an ex-member of the M.R. who had devoted herself to this work with the greatest enthusiasm from the day of her arrival and after whom the various methods of getting out Duds -- i.e. messages which for some reason do not decode on the message setting arising from the indicators, though in point of fact they were encoded on the key in question-- by juggling with the indicators were collectively named "Eppery". This section, however, only worked from 9 a.m. to midnight, and it was the responsibility of the M.R. proper to attempt to decode any duds urgently requested by Hut 3 during the night.

There were various methods of approach to the problem. If the dud was part of a message, the rest of which had been decoded, Hut 3 could often give a crib which could be tried on the rods. Failing this, the most likely reason for the message being dud was a morse error in the indicator, and the more probable alternatives could be tried. It was often possible to get indicator corrections, or other helpful information, from the log readers, but this involved a delay of about 24 hours. Again, particularly in part messages, the possibility of cillying was worth consideration. Or again the beginning of the text might have been missed, and by checking the numbers of letters it was sometimes possible to find the correct starting position. Often a comparison of the depths would show that a combination of the different texts would provide the correct decode. Nor did the above methods exhaust all the hand methods for solving duds adopted; but it was difficult to lay down any hard and fast rules for the breaking of duds, as

* The chapter on the Bombe in the technical volume should be referred to for an explanation of any terms about menus which are obscure in their present context.

each one had to be considered on its merits and a lot depended on individual initiative and perseverance.

[illegible] were also available if required. One or two of the bombes were fitted to take an attachment which would try [illegible], such as HIMS, in all positions of the text, and the [illegible] test the stops produced. The Arlington Bug-buster [illegible] dealt with a very good chance of success, but this was not placed able for very urgent duds, owing to the inevitable delays in the mailing to Washington. For fuller details of these and other mechanical methods of dud-breaking the reader is referred to the appropriate chapter in the technical volume.

1.72 FINAL SET-UP FOR BOMBE CONTROL

1.720 Connections

Before the installation of the tube system to Hut 23, and the teleprinters to the outstations, there was great congestion on the telephones. First stops had to be checked back on every menu to ensure that the menu had reached the outstation correctly; all wheelorders were telephoned to the M.R. by the i/c Ops. at the outstation, and at the conclusion of each job O.C.B. (O.C.Bombenlage) telephoned Controller in Hut 23 -- the Wren officer in charge of all bombes for the shift -- to tell her that the bombe could strip, and to give her its new job. In addition all stops were telephoned, and consequently the four, and later five, telephones were in constant use, and the two or three people who had to answer them had a rather harassing time. Bombe copies of menus had to be taken over to Hut 23, and this was quite an adventure at night; one moment one was ankle-deep in mud, the next walking into a concrete mixer left by the workmen engaged on building the new blocks. For several weeks there was a deep trench which had to be negotiated by a narrow mud-coated plank, and more than one person met a muddy fate at this point.

However, the tube system and the teleprinters made life a much easier existence, and a later improvement, saving a lot of time and trouble, was the checking of wheelorders by the i/c Ops. at the outstation, who informed Controller when a machine had finished its job. Controller then told O.C.B. that the bombe had stripped.

1.721 Routine Organisational Jobs

The routine organising functions for each shift were shared among the following individuals.

(i) O.C.B.

When told by Controller that a bombe had finished its job, she gave it a suitable new menu, remembering the idiosyncracies of some machines, such as dislike of double-input menus, lack of D-boards etc., and informed Controller what wheelorders had to be run. She decided in consultation with i/c Ops. in the Watch how many bombes were needed for each menu. The G.A.F. keys generally ran on the Kingston wheelorders, often reduced by the non-clashing and non-repeating rule, and the correct wheelorders for each job were worked out by O.C.B. The Watch Head of Shift advised when any particular menu should run more wheelorders, and the instructions were passed on to Controller. It was generally found more economical for the bombes on one menu to be taken from the same bay and in the case of delayed hoppity menus on the high-speed bombes a complete bay would be put onto one menu. Of course, with very urgent menus it wasnot always possible to keep the bombes together, and in these

[illegible] available ones were put on, regardless of station. [illegible] necessary with the ordinary bombes as they [illegible] frequent intervals.

A record was kept of the bombes with their times of [illegible] because of the new job and the time it was started. [illegible] W.R. kept a card for each menu, giving details of the card, number of wheelorders and the bombes running it [illegible] at a glance how the bombes were disposed, and [illegible] job.

(2) [illegible]

She indexed the menus in a card-index, numbering them consecutively according to the name of key and date, and marked the cards when a menu had failed. She made out stop-sheets for each menu as it was put on, writing the names of the bombes in colours, which were different for each station -- red for Stanmore, blue for Eastcote, black for the U.S.A. bay at Eastcote, green for Gayhurst, brown for Adstock and purple for the Hut 11A bombes. This made it simpler to find sheets quickly when stops came in. Key-breaks were reported to the Duty Officer, to the Decoding Room and the Registration Room, and, if current, to Control, and this member checked that the completed key was entered on the various cards and in the Watch and M.R. key-books. Another task was the keeping of a record for Mr. Knight of the time taken by each bombe to complete its job, and this in itself provided her main occupation.

(3) "TUBE STOOGE"

The bombe copies of the menus were sent to Hut 23 by tube. From there they were teleprinted to the appropriate outstation, and a copy of the teleprint was returned for the "Tube Stooge" to check against the original menu. She also had to check that the wheelorders were sent over correctly, and that details such as B or D reflector, C.S.K.O. if necessary were inserted. She received the teleprinted good stops, and after checking the Serial numbers passed them on to be written on the stop-sheets. After a bombe had stopped i/c Ops. at the outstation sent by teleprinter the list of stops which the M.R. should have received, and these were handed to the "Tube".

(4) "H III"

She checked that all the stops had in fact been received, that each one had been tested, and then filed the failed menus, with the appropriate stop-sheets attached. Another of her tasks was to keep a record of the returns necessary owing to machine faults (these were sent in as discovered) and to check periodically with Control that these had been done.

(5) "H SHOW"

This member wrote down the stops on the relevant sheets and passed them on to the testers. Stops from Hut 11A came by telephone to her, and first stops had to be checked back, as there was in this case no teleprinted copy of the menu. Any very good stop, which seemed likely to be the correct one, was also phoned to avoid any possible time delay, and this was written down in the same way as passed to the testers.

On night shift, or when the shift was short, it was sometimes possible to combine these last two jobs.

(6) W/T.CH.

This, the most important job of all, was strictly speaking, [illegible] but was performed by a member of the W.R. sitting in the Watch and working in close collaboration with the [illegible]. Under his direction she was responsible for the initial allocation of bombes to jobs in so far as this was governed by intelligence and cryptographic priorities. She kept a complete "legal" of jobs waiting, to be run arranged [illegible], and fed the jobs to O.C.B. according to the list of priorities and the instructions of Watch H/S. It should be noted that the [illegible] was concerned with keys, while O.C.B. dealt with bombes.

The logs gave a detailed record of jobs out, failed, running on [illegible] and i/c Cyp., kept the H/S in Air and Army Watch informed of the progress of their most urgent keys, reporting any breaks that occurred. She was also responsible for guiding those members of the [illegible] who were engaged in menu-making i.e. seeing that the jobs in hand were dealt with in their correct order of priority and any spare time she had from her primary duties she devoted to making up menus herself. In general, she acted as liaison between the Watch H/S and O.C.B.

1.1.2 Final Testing of Stops

Of the rest of the shift, one or two sat in the Watch to make up menus, and the others tested the good stops i.e. those stops that had successfully passed the initial examination conducted by the Wren testers at the bombe stations and were sent on for further scrutiny. At one time these became so numerous that steps had to be taken to reduce the number reaching the M.R. This was done by various means:-

(1) The basic menus were made slightly stronger e.g. a 9_3 was no longer run unless it could take C.S.K.O. and a 15_1 was run in preference to a 14_1.

(2) Whereas, previously, any stop with one contradiction had been sent over, it was decided that when the menu was made up on clean and well-duped texts only stops with no contradictions would be tested. Stops on unduped menus with one contradiction on an outlying link were still tested, to allow for the possibility of corruption.

(3) A system of "phantom links" was introduced. These were not plugged on the bombe, but were used by the Wren testers for checking, and stops which gave contradictions on these letters were not sent over. This was the greatest labour-saving device of all, and in spite of the objections of the pessimists (in other sections) who feared that the increased risk might result in the correct stop being missed, the Wren testers were by this time so efficient that this was never proved to have happened.

1.1.3 Special Problems.

Variety was added to the ordinary testing by delayed hoppity menus, which allowed for a turnover in the stretch, and by H menus (4-clousures run with queries instead of letters, and without diagonal boards, on keys where Enigma Uhr was suspected). The joy of testing those latter was that there were no confirmations to suggest a good stop, and any one might be the correct answer. Then this was found, the subsequent problem of finding the basic

stecker and ringstellung provided exercise for the more mathematically-minded. Occasionally, too, the M.R. helped with the breaking of a reflectors, and had the expected wholesale conversion to b materialised in January 1944, there was a trained team ready to take part in the mass hand-breaking attack.

A development which preceded the introduction of Enigma (the twice-daily change of stecker. The three periods were known as R, S and T -- period S having four stecker different from the original R, and T having four others different from S. The M.R. provided one or two people per shift to work on this problem and discover the correct variations. As a security device this was quite futile, and proved nothing worse than an annoyance. It fortunately did not last long, the Germans evidently finding it as much of a nuisance as Hut 6.

Although the major crises of Hut 6 did not affect the M.R. so directly as they did most other sections, there was quite an appreciable amount of extra work involved, especially towards the end, when two keys, particularly Army keys, became very confused -- partly owing to German security measures, such as the dropping of discriminants and the encoding of callsigns, and partly owing to the natural confusion caused by a rapidly moving battle. It was often impossible to identify a key until it was broken and decoded, and so some Army keys were run under a general name such as Barnyard (Western Front) or Aviary (Balkans), and only named when they had been subsequently identified. This meant that if a Barnyard came out, every other job on a Western Front Army key of that date that was running had to be tried on it, and if, as often happened, they all decoded, O.C.B. was flooded with as many as 70 bombes, all clamouring for new jobs. To get these all settled without too long a delay (one had always to have an eye on Mr. Knight and his bombe delay statistics) provided a hectic half-hour. Another irritating possibility was that the key might turn out to be that of the day before, and it was not unknown for someone to spend an hour or two on a difficult ringstellung, another twenty minutes or so writing out all the cards and entering the key in the keybooks, only to discover that it was yesterday's key which had been out all the time.

The introduction of CY into Army messages caused an added complication. This was a system by which the left-hand wheel was moved by hand in the middle of the message. The position was indicated by the letters CY followed by two consecutive letters, the first of these being the setting to which the wheel must be moved. Finding a ringstellung on one of these messages (and one was never sure whether or not the CY would appear) involved looking for this position. When found it provided the correct clip position for the left-hand wheel and was thus a help towards obtaining the full ringstellung, but if the text was corrupt, it was often difficult to tell exactly where it "went off". If the crib was at the beginning of the message, the CY position could be ignored, but if it was a signature (the majority of Army cribs were) it was essential to find this position and this was often no easy task.

The last few months provided such a large haul of captured keys that it almost a full-time job for someone to test them all, and to enter and report the breaks, and inevitably, as the war drew to a close, there was less and less to run, and bombes often had to remain idle for long periods, but, rather against expectations, the M.R. continued at almost full pressure right up to VE Day -- a more satisfactory finish than the gradual dying out they had been led to expect.

In conclusion, a special word of praise is due to the two American members of the M.R. It must have been rather disconcerting to them to be placed in a room otherwise exclusively female, and to have a girl in charge, but they never showed the slightest resentment, and proved most cheerful and co-operative workers.

CHAPTER 1·8

HISTORIES OF SPECIAL GROUPS OF KEYS

1·800 GENERAL INTRODUCTION

Throughout the war Hut 6 had a clear theoretical objective before it - to decode currently every message sent out by the Germans. This achievement being for long an obvious practical impossibility, it concentrated instead upon the traffic likely to give the maximum of assistance to the British or American forces engaged in the most important campaign of the moment. Thus the emphasis of the work shifted from one key or group of keys to another as the war progressed, the potentialities of a non-operational group not being overlooked, but the immediate requirements of the moment always taking pride of place.

In the following account of the breaking of individual keys or groups of keys some attempt is made to show the correlation between the Hut 6 effort and the demands of the war situation, and the keys are therefore described in the order in which they rose to their highest breaking priority. Thus Red, though the outstanding key for so many years, comes first because it provided high-grade intelligence in the Battle of France, and Brown, which became of supreme importance during the raids on Britain, comes next. And so through the campaign to the end of the war, the Eastern Front Air and Army keys coming last in the list because, although they had provided valuable intelligence for a very long time, they only became of immediate operational assistance to our forces when the link-up between the Eastern and Western Fronts was drawing near.

Finally, sections are included on some of the types of key not covered under the previous headings, such as the G.A.F. Y Service key Mustard, and the keys connected with the V-weapons. In all these accounts it has been impossible to do more than indicate briefly the main lines followed in the course of breaking. The story of Red, for instance, broken steadily for more than four years, does not indicate the anxiety which it often gave the cryptographers - there was a night in 1942 when six correct cribs failed to produce the right answer ! - or the general relief felt when the day came out.

Even so, not all the keys broken are described. The Norwegian keys, especially the Air keys Narcissus and Lion, deserve a separate section, if only to tell of the hard battle fought by the Qwatch against the increasing use of D on Lion in 1944. Osprey, the key of the Organisation Todt, broken on cillies so many times that Hut 3 felt compelled to detach an expert to read the traffic in spite of its uninteresting appearance; Stork, the key which caused a sensation in Hut 6 by decoding in Hungarian, and a problem in Hut 3 because no one knew the language; Dingo, the Geschwader key with a remarkable crib 300 letters long which only appeared once every teh days; these, with many others of short duration and minor importance, are omitted. But enough is said to show the general trends in the work of the cryptographic sections and the varying ways in which keys were broken.

1.801 RED

1.8010 Red : A Major German Blunder

In the opening chapters of this book it has been told how in 1940 interception was confined to Red frequencies because this colour carried an immense volume of traffic and was being broken. At that time Red carried practically all the Air Force traffic of any importance with the exception of the specialised matters dealt with by Brown. The only other Air Force keys were Blue, the practice key, and special keys carrying small amounts of non-operational traffic. Thus any G.A.F. communications of importance sent over the air were almost certain to be encoded in Red: and by breaking Red, Hut 6 could probably give warning of any new Luftwaffe move in any quarter. It was of course a cardinal error on the part of the enemy to use a general key of this type: apart from the obvious dangers of having too many messages on the same key, it meant that the insecurity of a single operator in, say, Norway might perhaps provide us with information of the employment of a new bomber group against Britain or of concentrations of planes for some new drive in the Balkans. As the war progressed the Germans introduced more and more keys which were designed to reduce the volume of traffic on Red and to increase security by the use of local keys: but the original error was never rectified and Red, the general Luftwaffe key, remained in use until the end. By this time it had been surpassed in urgency and importance by the keys dealing specifically with the Western campaign. But it was still of great interest as a potential source of information about the G.A.F. everywhere.

1.8011 Breaking, 1940 - 1945

The first war-time breaks of Red were made in January 1940 on the old indicating system. The change to double indicators before the Battle of France meant that hand methods alone could be used, for the first bombe did not arrive until August; but large numbers of cillies coupled with ringstellung tips given by inspection of first messages enabled many current breaks to be made even at this stage. The completion of the bombe and a reduction in cillying generally soon led to a shift of emphasis from cillies to cribs: and cillies soon became of very minor importance in breaking Red. Useful in providing wheelorder preferences when bombes were few, they occasionally gave us a day which had failed to come out by other means. There was, for instance, for some weeks an operator at Bari who used to cilli most of his messages and usually used the indicators ELF and JUN. One day was broken on a menu consisting of seven ELF's; but more usually the day was out before these cillies began to arrive, for the group normally worked only during the night, when it forwarded traffic encoded during the evening.

Red always provided plenty of traffic - 1000 a day during the Battle of France in 1940, sometimes over 500 in periods of simultaneous operations in the Mediterranean and in Russia in 1941 and 1942, and always over 100 even in spells of comparative inactivity. There was therefore usually in the absence of any strict cipher discipline in the G.A.F. a wide variety of cribs, and the problem was normally not to break the day but to break it early. Weather cribs were often valuable for they tended to come at regular intervals and frequently to report no change in standard form. The first Red crib to break a day, Keine

Zusätze, was a short message saying that there was nothing to add to a previous long report on the weather; and the tradition thus set was maintained by the Shorter Wueb, which broke over 100 days in 1941, the Lett Wett and Czech Wueb, great stand-bys which went over to Fliegerkorps keys in 1942, and the Skunk Wetter, a crib of 1943 so good that Red parents were heard wishing that it would return to Skunk whence it came because it made the breaking of Red so childishly simple. At one time or another every type of routine message sent by the G.A.F. was used as a crib on Red. There were operational orders like the famous pair sent out by Luftflotte 4, "Besan", i.e.

BESONDERE ANORDNUNGEN FUER DIE LUFTAUFKLAERUNG AM (Date of next day)

and "Befehl", which said

BEFEHL FUER DIE KAMPFFUEHRUNG AM (Date of next day)

Year after year these messages would make spasmodic appearances, in form almost invariable. On Red even when they were identifiable daily they were only used in the last resort, for they did not arrive till very late in the day - one more example of the strength of the Red crib position. Then there were Tagesabschlussmeldungen - one of them, Chef, had a long career -, tuners, and operational reports of all kinds. Of the latter the most notable were the reports from Fliegerkorps X, which for long provided several cribs a day, sometimes with depth on the address - these were the "Robinson Fun and Games" of which examples are given in the chapter on cribbery in the technical book. Of tuning messages those on the Jägerleitkreis were of the greatest value, for in 1944 when they came into prominence the crib position on Red was considerably weaker than before. There were several Jägersprüche a day, and though the variety of forms employed included ABSTIMMSPRUQ..... or simply Quatsch, there was usually one each day which began DAS IST EIN ABSTIMMSPRUQ.... From January 1, 1944, some of the Red traffic was encoded with Reflector D, but breaking was not seriously affected because there were always some cribs using B which gave a break into the successive D-periods. The Jägersprüche were particularly useful here, as they steadily used B throughout.

1.8012 Supreme Importance of Red

So Red was broken almost solidly from the middle of 1940 to the end of the war. In 1942, 1943 and 1944 not a day was missed and in 1941 a clean sweep was probably only averted by the compromise of Red in November, when for ten days hand keys were used instead, to the general confusion of both the G.A.F. and BletchleyPark. This compromise was no doubt one of the reasons for the introduction of Fliegerkorps keys on the following January 1st, an event which demonstrated for the first time the cryptographic hold which steady breaking of Red was giving us over the G.A.F. The new keys were broken on some of the old Red cribs which had now changed their allegiance; and in the following years there were many instances of new keys being broken on R.E.'s from Red or on cribs either transferred to the new key or occasionally sent in Red. Even after the opening of the campaign in the West, when the Luftflotte 3 keys, Ocelot and Jaguar, took pride of place in intelligence importance, Red remained supreme as the key most likely to lead to breaks of others by re-encodement. The direct intelligence value of Red must have been enormous; a steady stream of high-level information about the past and future operations of the G.A.F., with occasionally memorable messages on a variety of subjects like the routeing of the Bismark or the plans for

the invasion of Crete. Scarcely less important was its indirect intelligence or cryptographic value in providing the means for so many other breaks.

1.8013 Blue and Pink

Perhaps mention should be made of the two keys the most closely parallel to Red, both of which were of long duration and wide distribution, though Pink was confined to the most important commands. Blue, the Luftwaffenübungsmaschinenschlüssel, lasted from October 1939 almost until the end of the war. In the early days of the war the practice traffic was indistinguishable from the operational messages, and in fact before breaks revealed the distinction between Blue and Red, Blue was believed to be the operational key. As soon as the nature of the key was discovered it had very low breaking priority and was not touched at all unless there was some reason for believing that it might have more than its usual interest. In 1942 Blue was involved in key repeats and was therefore broken to give assistance with other keys. Later in 1943 some of the Cockroach traffic, including one crib, went over to Blue, and it was therefore broken by this means. Most of the Blue breaks were on cribs which had at some time passed on other colours, such as the Daffodil Zahlsprüche or the Snowdrop Tagesabschlussmeldungen; and it became a routine to break if possible a day a week to make certain that the traffic was still all practice. In 1944 Blue traffic totals were very high until D Day, but thereafter most units ceased practising; the key, however, was identifiable until 1945. It was in 1944 that the most remarkable Blue crib was discovered, the "Verena". This was a report on the work done by the pupils at the signals training school. Each unit sent one return per day, so that thus there were several different "Verenas", but they had the common characteristic of giving results in a figure proforma, the figures being encoded in a simple bigram letter for figure substitution. Thus a message beginning

VERENA VL CH VL UB VL QF TK CH RX VL CH SG QF QF VL
= VERENA X 1 X 6 X 0 7 1 5 X 1 9 0 0 X

where 1/6 is the date and 0715-1900 the time of working in the school. It can be imagined that this crib caused no little difficulty to the Machine and Decoding Rooms, who had to distinguish between the purely random letters given when the text "went off", and a string of meaningless letters when it was "on".

Pink, the Luftwaffenführungsschlüssel, was the key intended for messages of the highest secrecy sent between the highest G.A.F. commands. It was rarely used and always difficult to identify. Apart from odd days broken on re-encodements - it often happened that a Pink message was refused because the recipient did not recognise or did not possess this rarity among keys - there was a period at the beginning of 1942 when Pink was used both in the Mediterranean and on the Auto between Berlin and the Russian Front. It was broken on an ex-Red crib, and provided for a day or two the very interesting message known as "Weisung", Berlin's daily orders to the Air Force governing the conduct of operations on the Eastern Front. In 1943 when the "Meldung", a long established Red crib giving the daily report of the German Intelligence organisation in Sofia, went over to Pink it was usually the only message in the key: but it enabled us to break one or two days when there was other traffic. Later the same year Kesselring showed a marked tendency to use Pink instead of Red for his high-grade messages, and a number of

days were broken on re-encodements and routine Army reports such as the "Limbo" (Lage im Bereich Oberbefehlshaber Südwest) which tended to be forwarded for information to the Air Command. This was the last period in which Pink was regularly identified with certainty: twice afterwards keys appearing on the G.H.Q. Auto were called Pink, but the likelihood is that they were not the Führungsschlüssel.

It was surprising - and fortunate for us - that no greater use was made of this key, for according to the instructions it should no doubt have carried all the Geheimekommandosache traffic which passed in Red. Red was stated to be "for secret and open matter", but actually a large volume of "top secret" traffic occurred in it also. Pink scarcely ever became fashionable in the G.A.F. Its imposing German name made it a sort of El Dorado to Hut 3, who found it difficult to believe that the Golden land had been reached when breaks decoded so little. But it was in line with German stupidity to give two keys, Pink and Red, a general distribution, and use one of them constantly, the other scarcely at all.

1·802 BROWN

1·8020 Introduction

In the days before the spectrum was exhausted and keys were still given colour names, Hut 6 made its first acquaintance with the Group that was to become a byword in Enigma history. The Brown cipher clerks demonstrated conclusively that the Enigma machine is only as secure as the men who use it. For it is difficult to think of any rule governing the use of the Enigma or, indeed, of wireless procedure that was not broken regularly by the clerks and operators of those Abteilungen of the L.N. Versuchs Regiment which used this key. Although the Group was known to the intercept stations very early in the war (some reports say before the war), it was not until the end of August 1940 that the attention of the cryptographers was drawn to the increasing traffic totals on Brown, which could be discerned amid the subsiding floods of Red traffic. As was soon proved, Brown was not a key capable of putting up much resistance to cryptographic attack and September 2nd Brown soon capitulated to the bombe, setting the widespread speculations about its content at rest.

The Brown Group was found to consist of a number of French stations, whose staffs were engaged on directing wireless beams for beam bombing by K.G.100, and several German stations, where the original experiments on the subject had been carried out and where research was still in progress. As the war went on, this German group with control at Köthen (headquarters of the Regiment) proved a constant factor in a Brown picture which was always changing with the ephemeral appearances of other stations. The German stations supplied a continuous thread, linking the early beam bombing experiments with many other technical developments culminating in the V1 and V2 trials.

Since the Brown Group remained a compact wireless network separate from the other networks of the G.A.F. signals organisation, and as a break of a Brown key often depended on knowing the personnel of a particular station, it was only natural that a more personal interest should be taken in Brown than in other keys. The facts that traffic totals were small, so that every message was necessary, and that hand attempts were possible on Brown, long after most other keys had become cilliless, accentuated the interest. This history of the L.N. Versuchs Regiment as seen by a Brown cryptographer enters more into detail, perhaps, than the other key histories, in an attempt to convey the atmosphere and approach which seemed most suited to achieve the best results on Brown. Here then, is not only the struggle to break the current operational key (Brown and Brown II) but also the efforts to maintain a hold on Brown I through a dull intelligence (though interesting cryptographic) period so that new inventions should not take us unawares. Probably any new Brown key could be broken in time, if there was any volume of traffic, but by breaking Brown I regularly, new keys could be broken quickly. It is at the birth of a new weapon when experiments go wrong, that most information about its mechanism is given, and not when the initial difficulties have been overcome and only the extent of its power remains to be determined. For this reason, it was important to break any new Brown keys as soon as they appeared.

After August 1943, the activities of the Brown Group were divided between two opposite ideas - the one of attack, and

the other, defence. This period to the end of the war is covered by the story of Brown III.

1·8021 "Target for Tonight"

Phase I : September 1940 - May 1941

The story begins during the period of the first Blitz on Britain, September 1940 to spring 1941, which was the most exciting and momentous time in Hut 6 history. After the famous "Few" had swept the skies of Britain clear by day, Hut 6 played its part in the task of rendering those skies as hazardous by night. Although this is not the place for a description either of beam bombing or of the way our knowledge of it was built up on the information given in Brown, some facts are necessary so that the background to the work of the Hut can be understood.

The Luftwaffe used K.G.100, flying along wireless beams, as a pathfinder group to indicate the target area for the other bombers. This was K.G.100's main task, although occasionally it carried out special operations on its own. Each evening of an operation, the directions for the setting of the wireless beams for the target were sent out in Brown from the headquarters of K.G.100 at Vannes to the beam stations at Boulogne, Cherbourg and Morlaix. It was Hut 6's job to send these instructions, decoded, to Hut 3 in time for action to be taken on them. Only if that vital information arrived in time, could the slender resources of night fighters and anti-aircraft guns be utilised to their fullest extent and concentrated on the small area through which it was known the enemy planes would pass. Later in the Blitz, when the technique of jamming and bending beams had been developed, it was even more important to have this information.

As most raids took place in the early evening, just after dark, the time factor was constantly in the thoughts of the cryptographer and a sense of urgency, such as was never felt again, permeated the whole Hut. For, never again, was the battle so close that the results of one's work had an immediate personal interest, when the difference of an hour in breaking time might mean the difference between life and death for some inhabitants of this embattled island. As the target had to be worked out from the beam settings, it was important to break every day so that the number and directions for the target were known for future reference, even if the day could not be broken in time to be of current operational use. Sometimes there would be no Brown traffic until after midday and with the then shortage of bombes, the importance of picking the right version of a crib first time was paramount. It was about this time that the first decisions on bombe policy had to be taken, to run an early crib on 60 wheelorders or wait for cillies to reduce the wheelorders, thereby allowing other keys to be run on the bombes. These decisions depended on how good the early crib was, and what keys were waiting to be run.

Now, any daily set of orders generally became stereotyped in the German Signals Organisation and Brown was no exception to this rule. The cribs on Brown were all connected with the beam bombing and the phases of a night's operation could be followed by the cribs. Let us take for an example of this a day in December 1940. The beam stations were warned of an operation that night by a message (known as 'Vorbereitet Betrieb') about midday giving the number of the target and notice whether there would be one or two operations. About two hours before the beams were due

to be switched on, the detailed instructions on directions etc., would be transmitted; these, the beam stations concerned would have to re-encode and send back to Vannes as a check that there had been no corruption in the first transmission. The beams were then directed and switched on, and a report to this effect ("Fertig Eingerichtet") was sent back to Vannes from each station. There was then an interval while the operation proceeded and should the day not be broken before the next crib came in, it would be then too late, for this crib was the "Betriebsschluss" to tell stations that all was over. The final cribs in the series were the reports of the beam stations on the night's activity generally consisting of that original German phrase and cryptographer's friend, KEINE BESONDEREN VORKOMMNISSE. These messages, known as Boller's Betrieb and Johannssen's Betrieb (the latter, one of those men whose name no two cipher clerks spell the same), were often sent out early the next morning and were the cribs that gave rise to the headaches of bombe policy. This sequence of recognisable messages would be altered by another operation that night, and would be replaced if there was to be no operation, by a short (usually 32-letter) message which would give us as well as the Germans this information. The other occasion when the cryptographers could tell what a message was about, without decoding it, was when there was a slightly longer message than KEIN EINSATZ the night after a raid. This would be HEUTE ZIEL WIE GESTERN and, as the Germans quite often raided the same place two nights running, a watch was kept for this message the night after a new target had been raided. The Duty Officer would inform Hut 3 if either of these two messages came in when the key was unbroken.

On December 12, 1940, a discovery was made which practically halved the bombe time needed for Brown. This was the famous stecker rule, which lasted on and off from October 15, 1940 to July 15, 1943 (Brown key months ran from 15th to 14th). Here it must be explained that the Brown keys did not follow the rest of the G.A.F. keys in having ten stecker per day, but only had six or seven. There was thus always a temptation to pair the days so that letters steckered on one day were unsteckered on the other, and to a neat and orderly German mind, this must have been irresistable. Anyway, the compiler of the Brown keys (who was one of our best aids to breaking) succumbed to the temptation. After one day had been broken, the pair day could usually be rodded out, or a hand attempt made much easier. The very fact of there being twelve or fourteen self-steckered letters every day was a great help in hand attempts and was responsible for a new technique of breaking - "the clonk". Roughly speaking, each constatation of a crib (of known machine setting such as cilli or cilli and signature) and encode was assumed self-steckered in turn and machine positions were examined to find the one with the largest number of these self-steckered pairings. On the paired day the actual self-steckered letters were known so that positions could be rejected which did not give the required pairings.

After this stecker rule was found, most Brown days were broken, and from the information gained the subtle method of bending the beams was developed so that German airmen bombed open fields instead of towns without realising their mistake. By the spring of 1941, the Germans had become very suspicious about these counter-measures and the speed with which they had been prepared, and a great security drive was launched. Fortunately for Hut 6, no one thought about wireless security and we were able to read how all the past records of the German technicians had been checked and about the wild fantasies the

Germans had, of Allied agents signalling the target for the night across the Channel. When the invasion of Russia was imminent, the Luftwaffe withdrew its bomber squadrons from France and the first beam bombing attack had been withstood. The German scientists then retired to Germany to think again and to prepare for the second round safe, as they thought, from prying eyes and ears.

Phase II : December 1941 - June 1942 : Brown II

The results of these second thoughts began to appear in December 1941 when the Brown traffic, which had remained negligible and unbroken for the preceding five months, increased in volume and showed the key had split, presumably for security reasons. Communications about the experiments in Germany were passed in one key, named Brown (G) and the French stations used another, Brown (F). Such simplicity in naming, however, was contrary to usual practice and these names gave way to Brown I and II respectively. The trials in Germany of the modification of the method of beam bombing followed much the same pattern in the sequence of cribs for an operation as the winter before, and the old routine of cribs, cillies and clonks was soon in full swing again. Because of the natural close liaison between experiment in Germany and preparation in France, re-encodements were often found between the two keys and Brown was in a healthy enough condition in January to be returned to the operational shifts as a current commitment. In February, the Brown keymaker evolved another delightful method of compiling keys. This was to add one to each component, (wheelorder, ringstellung and stecker), of the key of one day to get the next day's key. Unfortunately, these "stepping" keys were on Brown I which was easier to break than Brown II and they only lasted a month. It is perhaps as well that the bombing operations were not on the same scale as the previous year as the breaks on the operational key were not so frequent as before. This was due not only to the two separate keys, but also to the fact that less traffic was being passed between the French stations. Still enough was broken to help the counter-measures, and raids became too costly to a Luftwaffe whose wings, stretched from Moscow to the Atlantic and from the Arctic circle to the Egyptian desert, were weakening under the strain. At the end of June, the beam bombing stopped, the Brown II traffic sank to an unbreakable level, and Brown went back to Research.

But there was still one last kick left and at the beginning of October, after an initial break on cillies, a few more days were broken on Betriebsschluss (once or twice the only message), but there were no other signs of operations in the traffic or, indeed, always in the air activity over this country. This last mystery was coupled with a ten stecker key and so it was without regret, but perhaps with a sigh for past glories, that the cryptographers said goodbye to a key which had been the most important key broken in Hut 6 and was now only a shrunken remnant, often rescued from the "no colour" by a watchful parent. The beam stations were used as radio beacons for homing aircraft for a few more months and were then dismantled, the final farewell to a secret weapon which had only failed to secure the results it promised, by the lack of cipher security in the men who used it.

1·8022 The Lull : Brown I

As has already been related above, Brown I was used by the stations in Germany for the experiments in beam bombing. When these were finished, the content of the traffic became purely administrative, and while cryptographically it was a most

interesting key, the effort and time expended on breaking it was only justified as a long term policy of keeping in touch with the Versuchs Regiment which was sure to be connected with any new weapon of war needing wireless.

The German stations remained a nucleus of the Brown I network until overrun by the advancing Russian armies, and added to this nucleus were stations in occupied territories, such as Paris and Kharkov. Also, from time to time, stations would be set up in places convenient for specific experiments and then disbanded when these experiments were completed. After a scarcity of breaks during the summer of 1942, a firm hold was taken on Brown I in September, which was not shaken off until the next autumn when, with the arrival of Brown III and IV, less time could be spent on Brown I.

There were mostly small stations on Brown I, and in each case the staff consisted of an N.C.O. in charge and a few men. All would take their turn at encoding and decoding messages, besides operating the wireless set, and with no activity at night only two shifts were necessary. Their customary practice, thoroughly approved of in Hut 6, was to use the initial trigrams of their names as message settings for any Enigma messages they encoded and as signatures when chatting over the air. Nor was this the limit of their helpfulness, for the N.C.O. would sign all the messages so that unless, as once happened to our annoyance, an officer or higher ranking N.C.O. was visiting the station, the signature to messages would be constant and message settings limited for periods up to three months. Then there would be a General Post and another N.C.O. and party arrive with a new signature and series of message settings. Often advance notice of any change was given by the operators enquiring in clear when they were to be relieved. In order to pass all such information, which could be obtained from the logs, to the cryptographers, a daily Brown "Story" was instituted early in 1942. This was compiled by the log reader and included a list of messages (with receipts) with the account of the day's working as well as any "Klartext". The Brown story was originally intended to help the breaking of Brown II and as a check that all Brown II traffic was seen by the cryptographers. Such a check is invaluable where the volume of traffic is small and one extra message may mean an extra cilli and perhaps another break.

With the limited choice of message settings, depth reading was quite a common exercise, made easier by the routine addresses used. For, apart from communications and apparatus tests of which notice would be given in clear, most messages were about the three fundamental interests of the serviceman, common to every nation - pay, leave and supplies (cigarettes, chocolate, etc.) For example, about 90% of the messages from Wustrow in early 1943 would begin in one of the three following ways:-

R E Q N U N G S F U E H R E R X X (Pay clerk - Pay)

O B L T X X L I C H T H A R D T X X (O.C. Company - Leave)

O F W X X P E T R I X X (Sgt.Major - Supplies)

and have one of the three message settings HEL, GRI, STE. The double X's also illustrates one of the peculiar types of punctuation which were used at different times on Brown. After some glaring examples of misencoding, a new punctuation system would be laid down: at one time this consisted of putting a "Y" between

each word. This last system was never very popular and gradually dropped out of use, although one or two operators kept it up long after the others much to our disgust as this meant more versions had to be run.

Most days were broken on cilli plus signature menus, if there was no ringstellung tip to make a hand attempt possible or if the constatations were unfavourable on a paired day for rodding. The amount of traffic passed, except at the end of the month, was very small and there was usually not enough traffic for the Brown cipher clerks to give us enough cillies for a menu. When Brown I had to be run on the bombe, its low intelligence priority handicapped it in the competition for bombe time, although it is only fair to say that, at first, it basked in the reflected glory of Brown II. Later, Brown I days were only run if there was a reduced whoelorder and one menu of cillies or cilli plus signature. Thus the right signature had to be found first time, which eliminated Köthen signatures as these were many and varied.

At the end of each month each station had to send in three reports to Köthen and this, on Brown, meant three cribs. The first was a list of wireless apparatus at the station, which only varied from month to month in the items out of action. The others reported

"Belegung über Sabotage, Spionage, und Funkdisziplin durchgeführt".

"Waffenappelle durchgeführt. Alles in Ordnung".

It seems inconceivable that any Brown N.C.O. ever thought about wireless discipline, never mind checked it. The most delightful piece of depth ever on Brown (enshrined in the appendix to this chapter), occurred when Unteroffizier Curth, then at Wendlestein, used CUR as a message setting for all three messages. The result was that it was possible to read the two shorter messages completely and the first hundred letters of the equipment return.

There are many such interesting episodes on Brown, every station producing some tit-bit at one time or another. Oberleutnant Heuterkes, in charge of the Brown station at Kharkov, used a special Sonderschlüssel, Brown "S", for sending personal messages to Köthen. Every day the same key was used and this lasted from October 1942 to January 1943, in the course of which occurred the longest cilli subtraction on record. A message with setting DOF at 1800 hours on one day was followed by the next message at 0900 on the next day but one, an interval of 39 hours. Then there is the station at Frankfurt, set up in 1943 to listen for Radar transmissions from British bombers. Every time there was an air raid near Frankfurt a report was sent in to Köthen of what had been heard. As this was generally a long part message cillying between every teil, a keen interest was taken in Bomber Command's operations.

Once, a simple substitution cipher was used by the Brown operators to send personal messages to each other and although disguised as Enigma by means of dummy indicators, it was soon recognised in its true colours. The use of IB (lieber) as an initial bigram and other abbreviations from amateur wireless procedure held up the breaking but the valuable intelligence that most of the operators were short of cigarettes was not kept from Hut 3 for long. This story has an amusing postscript - for, after some days had elapsed, an enquiry was made of the Brown parent whether it was thought the request for cigarettes was genuine. Apparently there was a group in Holland who were using cigarettes as a covername for some type of weapon, and the enquiry was to see if Brown could be connected with this group.

All idylls come to an end some time and after a record week of eleven breaks in July 1943, July 15th was broken and produced ten stecker. This immediately reduced the number of possible hand attempts. for the clonk method was valueless on ten stecker, which also ruled out pair days. The full seriousness of this situation was not felt at once, for a temporary easing of the bombe situation enabled more Brown I to be run on the bombe than before. So Brown I was broken regularly until October when, with the advent of Brown III and IV, all Brown bombe time was spent on these keys, only a little time being spared to run good cilli stories on Brown I. After October, Brown I dragged on a miserable existence, which even a key repeat in February 1944 failed to enliven, until the Russian armies advancing across the Elbe, and the American armies approaching Köthen wrote finis to this chapter.

1-8023 Attack and Defence

Brown IV

This is the brief story of another Sonderschlüssel. Oblt. Heuterkes and his Brown "S" have already given one example of how it is possible to break a key in use over a long period, by accumulating cillies from different days. The next example of such a key was Brown IV and here the reward for patience was much greater. For Brown IV was a key used between Brown technicians who had been lent for experiments connected with V2 and although no secrets about V2 were revealed by the Brown operators, presumably because they did not know any, the information they gave about trials and the men concerned in these trials helped to fill in the intelligence picture. The key used only one discriminant and, thanks to the regular breaking of Brown I, the cillies were recognised as those of particular Brown operators. After a week of collecting cillies, the key was run and came out and the messages could then be decoded as they arrived, the only worry being to make sure that the two or three messages a day did not get lost in the sorting.

Brown III

The policy of hanging on to Brown I was again justified when a new key, Brown III was introduced on September 15, 1943. Some stations in Western Germany which went over to the new key, had passed traffic on Brown I and the information gained during this period was instrumental in breaking the new key quickly. This Western Kreis with control at Köthen, was joined in its use of Brown III on October 15, by a Baltic group which had been using Brown IA, the key of the previous month's Brown I. These two groups had nothing in common except the key and an allegiance to Köthen. The Western stations were helping to defend the Reich by plotting the paths of British and American bombers while the Baltic groups were testing out the weapons with which Hitler still hoped to pluck victory out of defeat.

The Western stations that were actively engaged in Radar work, besides reporting courses to the nearest fighter groups, also sent long reports to Köthen. These for some time were sent in a code without being enciphered in Enigma and were dealt with directly by the section of Hut 3 interested. From January 1944, these stations sent their reports in Enigma and this, of course, meant cribs. The series of cribs were called, picturesquely, "Life at Cuxhaven", "Tales of Hoffman" and "Schmitz's Blitz", the last two being named after the men in charge of the respective stations. Not only could the beginning of these messages be used,

ERFAHRUNGEN VOM (date) but, as the reports were based on a proforma, the end could be used as a crib; for the answer to the seventh and last section of the proforma was always "Nein". Apart from these cribs, one Feldwebel, to wit, Schützendübel, possessed a name, long enough with his rank to run as a delayed hoppity. In fact, later in the year, after Brown III had been unbroken for some time, an initial break was possible because an operator querying a signature, received "Schützendübel" as a reply. This was run assuming a promotion which had been thought imminent the last time the key was broken, and out it came.

There were a few stations on the Western Kreis not on operational work and one of these, the station at Erfurt under the command of Lt. Gauss, provided a large proportion of the breaks during the period of its existence. The trials at Erfurt involved the use of an aircraft and this led to the only weather crib ever seen on Brown being sent daily to Köthen from Erfurt. While there was no point in refusing additional aid, the fact that most messages from Erfurt were addressed ANX EINSVIERX KOMP and the others ANX EINSFUENFX KOMP and all messages signed by Gauss, was generally enough in itself to produce top and tail menus. The favourite message settings of the operator encoding these messages were SCH and HAU which he used in that order, so that after a cilli to SCH could be assumed a message setting HAU. All the operators used the initial trigrams of their names in the old Brown tradition; one day was broken on seven OBE's; on another day, apparently overjoyed at being allowed to encode messages for the first time, one operator used CLA ten times !

For testing purposes, V1's were fired off from Peenemünde into a stretch of the Baltic and their courses were plotted by a series of Brown stations situated along the Baltic coast near Stolpmünde. These stations, known by their code names of "Spinne", "Ameise", "Fliege", "Hornisse", etc. were commanded by Lt. Mütze, familiarly called "Hut" by his friends both here and in Germany. Lt. Mütze spent a lot of his time travelling round the stations and as he would sign any messages emanating from the station he was visiting, it was important to keep track of this peripatetic Hut. As all Brown days were not broken, we had to supplement the announcements of his movements in decodes by references in log chat and it was rare for a Mütze signature to turn up at a station where it was not expected. Signatures were extremely important on Brown keys and it was pleasant to find another man whose name was long enough to run on its own. The Baltic counterpart to Fw. Schützendübel was Fw. Klüssendorf who was in charge of Fliege and also deputy to Hut.

The star operator in this Kreis was a man at Spinne who used LFG as outside indicator and DER as message setting. As Spinne acted as link station between the Baltic Kreis and Köthen, appearing in both groups, this operator had the task of passing on messages to and from Köthen. One week, he decoded all the messages he received on one star and re-encoded them in the same key before passing them on in the other star. This would have been a good security and camouflage measure, had he not set his seal of LFG DER on all the re-encoded messages.

The Baltic stations, transmitting on frequencies in the 3000-4000 band, were always difficult to intercept * and various "Black Market" sets were obtained to get down clean texts both of the messages and the non-Enigma traffic passed as well.

* Once an operator remarked that his interception was hindered by "the sound of running water".

These sets were either at stations not normally intercepting Enigma or were above the quota allotted to Enigma, and not obtained through the usual channel of Control Room. It is rumoured that there were one or two operators in Sweden taking this traffic, but whatever the unorthodox measures adopted, the distressing tendency to find cilli messages without any text to them was largely cured. Both Western and Baltic groups passed non-Enigma traffic (generally figures-letter code of plots and reports), and as this began to go astray because Hut 6 only received Enigma messages, the step of labelling all traffic on Brown frequencies, "Brown Sexto" was taken, and all such traffic was sent to Hut 6, where the Brown parent sent on to Hut 3 the messages that were not Enigma.

The fact that Brown III had ten stecker did not prevent the keymaker from trying to help us. From October 1943 to March 1944 he only used thirty sets of self-stecker, each set being associated with one or two wheelorders, or permutations of those wheelorders. Thus it was possible to run a weak menu, by assuming a set of self-stecker and running it on the wheelorders associated with the self-stecker. The sight of 96 wheelorders written on a menu, when 60 was the limit for Hut 6, was a little startling at first, but successes were achieved by this method on days that would not have been broken otherwise. In April and May, the keymaker went one better by repeating the February and March self-stecker respectively day by day.

About this time, with cribs on the Western Kreis, cillies and signatures on both groups, and helped by these self-stecker curiosities, Brown III seemed to be in as healthy a condition as a key could be on that amount of traffic. Yet, before a month had passed, the cribs had gone, traffic and so breaks decreased, and that annual disease of summer sickness crept over another Brown key. It was broken occasionally throughout the next six months and survived the destruction of the Western Group by the Allied armies and the transplanting of the Baltic Group to Denmark where they continued their experiments until VE day. By February 1945, Brown III was being broken regularly again, but the Brown keymaker was not to be thwarted in his desire to help us. As the March Brown III key, he copied out the Cockroach key for February, leaving only three March days to be broken by an ungrateful cryptographer.

1·8024 Conclusion

The preceding sections have shown how the Brown operators and clerks were completely lacking in any sort of security and how this was the only reason that Brown keys could be broken so consistently on such a small amount of traffic. One section in Hut 3 was accustomed to grade keys by their intelligence density, each message receiving some mark for the information it contained. The intelligence density was not always very high on Brown, but the cilli density certainly was, especially the day when there were eleven cillies in fifteen messages. One further example of this total disregard of all regulations is given by the procedure in the case of a message being wrongly encoded. If only part of the message was corrupt, the clear text of the offending part would be sent, giving a crib. If the trouble was wrong wheelorder, ringstellung or stecker, so that it was indecipherable at the receiving end, the encoder would adopt one of two courses. If he could find out what the trouble was, he would explain this in clear to save re-encoding the message. As this was usually in the form 431 NN . . . . . 451 CC for a wrong wheelorder, the correct

wheelorder was given to us as well. If forced to replace the message by pressure from the other operator, the same message setting would be used and any stecker trouble could be deduced from an examination of the two messages.

Why was it then that there was no cipher security on Brown and that this was not noticed ? The first reason is simply that the Brown operators and cipher clerks were not primarily concerned with this part of their job, but regarded it as a sideline to their experimental work. The fact that it was a Group on its own with little contact with the other G.A.F. signals units led to there being no change in personnel. No operators were posted away and the only newcomers in five years of war were the L.N. Helferinnen who caused more log chat, not less. The operators always knew the recipients of their messages and chat, and were not afraid of official interference. The officers were all more interested in science than discipline and Oblt. Lichthardt, O.C. 14 Kompanie, after his promotion from the ranks still liked to operate a wireless set and sign himself LIC. Small wonder then that lesser ranks were not afraid to chat happily over the air with such an example before them.

As the work the Brown technicians were engaged on was so secret, it must be presumed that no security officer was allowed near the Group, and, no doubt, the small volume of traffic that was passed rendered it safe to minds obsessed with fears of depth from quantities of traffic.

Perhaps the final comment on this lack of security is given by the news that all the records and files of the Brown Group had been destroyed by the time Allied units reached them. This must be a classic example of locking the stable door after the horse has gone.

Brown provided valuable information about beam bombing in 1940 and threw light on V1 early in that terror weapon's career, yet, to one looking back on five years of Brown, the most interesting thing was the way the characters and lives of the ordinary cipher clerks and operators were revealed by the indiscretions they committed and the information they provided.

1·8025 Appendix : Example of Depth in Brown I

On April 30, 1943 an operator at Wendelstein used his favourite indicator CUR, for three messages. From our knowledge of the monthly cribs it was possible to read in depth as follows:-

```
X K B B V D P K A D X E L H V O C T X U E E T S
S A R A M Y U N D Y K W Y E M I L Y A N T O N Y

V D S F B N P K V D H W U H Q T H J V H K Y S I K
B E L E H R U N G Y U E B E R Y S P I O N A G E Y

D O I W H Q - W R M Q P I E N G A Y C K A K N I K
A N Y O B L T Y L I C H T H A R D T Y B I T T E Y
```

1.3.5 THE MEDITERRANEAN AIR KEYS

1.3.5.1 General

It was along the African shore of the Mediterranean that Britain had to fight back against the Germans. Libya was the testing ground for the skill of British commanders and the perseverance of British troops. And from the fall of France to the few months before D Day, the Mediterranean was the central Allied operational zone.

The effect of this disposition of forces on the work of the cryptographers was to focus attention for many months on a batch of important Mediterranean keys. Particularly in 1942, when the work of Hut 6 was vital in covering the tank battles of the Western Desert, and when the resources of Hut 6 were inadequate to cater for all needs, we had to concentrate all our attention on the African war complex in much the same way that we had to concentrate on Red alert during the Battle of France. Research keys often had to be sacrificed to meet more urgent priorities.

During 1943, the resources of the Hut grew extremely rapidly, and both the Mediterranean picture and the other war pictures could be viewed more carefully. 1943 marked the climax of the African campaign. On January 23rd, our troops entered Tripoli, and by May 13th the last Axis forces in Tunisia had surrendered. The African campaign, which had ended so successfully, led naturally to the campaigns against the European mainland. The work of the cryptographers was focussed on those keys which dealt with the Allied invasion of Italy. 1944 saw the liberation of the Balkans and the firm establishment of Allied power in Italy, but just as the Allied capture of Rome on June 4th was overshadowed by the landing in Normandy two days later, so inside Hut 6 the emphasis on the Mediterranean keys was eclipsed by the rise of interest in the Western Front keys. In the days after D Day, it became difficult to summon great enthusiasm for some of the surviving Italian keys, particularly when Puma, the most important of them, went over to Reflector D and eventually Enigma Uhr as well, thereby producing a crop of technical difficulties.

In 1945, only one Mediterranean key, Leopard, was broken regularly, but its intelligence importance was low, and there was little excitement or interest in its exploitation.

The best way of describing the long attack of Hut 6 against the Mediterranean keys is to divide the story into phases, many of which are quite distinct, and can be treated chronologically. This account is divided into 5 sections:

1. The Triangle
2. The African Campaign
3. The Italian Campaign
4. The Balkans
5. The Last Months

The fourth section on the Balkans is not chronological. That is to say it covers a long period in itself, which, while part of the Mediterranean story, is best treated as a unity. It seems natural to leave it almost to the last for simplification, though the close integration of the Balkans in German Mediterranean strategy, particularly during the African campaign needs no emphasis.

1.(3) Brigitte

Before the beginning of 1942, Light Blue (German name - Brigitte) was the main Mediterranean Air key. It first appeared in January 1941 as an offshoot of the general Red key, and was broken for the first time on February 28th. Its main content was Western Mediterranean, especially Sardinia and the islands, and traffic passing to [illegible] in Rome. The arrival of Axis troops in Africa gave the key a wider application, but the German campaign in Greece (April 6th - April 27th) was mainly covered on Red. There were frequent re-encodements from Red to Light Blue throughout this period, which were very valuable in giving experience of how to deal with this new approach to key-breaking. At the beginning of 1942, Light Blue split into Gadfly (Fliegerkorps X) and Red. A third key, Primrose (Lgau.Masch.Schl.West) also made its debut. Together these keys [illegible] convenient triangle for the concentration of cryptographic effort. There were re-encodements between all three keys, particularly "Taxi" re-encodements, (messages referring to the arrival or departure of aircraft), which had passed in Light Blue during 1941, and now passed to Athens in Gadfly, to Rome in Red, and to Africa in Primrose. Earlier still there were Vorausmeldung re-encodements, passing on all three keys, and many sporadic re-encodements between two corners of the triangle. The triangle was linked at first not only by re-encodements, but also by stecker repeats. The crib position was thin, and difficulties of interception added to the problems of breaking these keys operationally. Primrose began as it ended with a crop of Abstimmspruch messages. It soon acquired in addition Flak messages, which remained one of its characteristic forms of expression. Gadfly inherited a Light Blue crib, "Chaven," but was always difficult to deal with from a crib point of view. Recce messages on both Red and Gadfly soon became the standard form of entry.

This original triangle did not take long to break up. In April 1942, Primrose split into Primrose (Lgau.Masch.Schl.Süd) and Snowdrop (Lgau.Masch.Schl.West), and, later in the same month, Gadfly split into Gadfly (Fliegerkorps X) and Scorpion (Fliegerführer Afrika). Gadfly continued to deal with the Aegean. Scorpion became a key of high importance and urgency, having many links with army groups. This complication coincided with the final crisis in North Africa. On June 21st, Benghasi was captured by the Germans, and three days later they advanced fifty miles over the Egyptian frontier. On July 1st, they captured El Alamein. Against such a setting, and the story of British recovery, beginning with the appointment of General Montgomery to the Command of the Eighth Army on August 13th, the African keys assumed an enormous importance.

1.(3)(a) The African Campaign

The main flow of German intelligence in Africa came from the Army keys. By comparison, Primrose was of very low operational priority, and methods of breaking had to be adopted which would throw least strain on the bombes. Scorpion, however, was important not only for its general information, but also for its re-encodements, particularly the invaluable Panzer Meldungs, sporadic on Scorpion, but regular on the Chaffinches. Luckily the breaking of the Scorpion was not dependent on its very inadequate cribs. Key repeats from Primrose, coming month after month, provided a providential way in. It was always difficult to fill in the missing days. Some idea of the concentration of bombe time on the Mediterranean keys during this period can best be given statistically.

In one week, the week ending November 21st 1942, Red, Primrose and Locust took 4403 bombe hours, almost half the maximum number of hours available for the total work of the Hut. The concentration of bombe time could have been even greater had it not been for two things, first the key reports, second a spurt of re-encodements from [illegible]. Short reports on the condition of aerodromes, re-coded from Red to Primrose, were found in September 1943 to [illegible] a simple June code, which could be broken almost at sight. The Naval Room was given a copy of the code, and then had the pleasant task of trying to fit the short June Reports to the length of the Enigma messages.

New grade ciphers were of great value in helping to consolidate the position of Locust, the key of Fliegerkorps II, which rose from a Research key to a key of high operational urgency, with the increasing U.A.F. activities in Sicily and the Western Mediterranean. At first it had been of interest for its accounts of German attacks on our Mediterranean convoys, but its intelligence became more general. Synoptic weather messages, coming regularly at all hours of the day, made Locust easy instead of difficult to deal with. The figure content of the messages could be given in part at least by the Meteorological Section. Even after these Synoptics had become less satisfactory, another excellent figure-code weather crib,"Three G.F.C.", enabled us to break many days. This crib is worth describing in detail. It started off with DREI, followed by the first two figures of the German Time of Origin (e.g.05), usually followed in turn either by OOXOO or 70X0. This consistency was maintained by reason of the stability of the Mediterranean weather. These two cribs were soon joined by yet more weather messages, Erika and Pantellaria being the chief, and a combination of both, known as Pantelka.

Re-encodements between Red and Primrose and between Red and Locust came steadily throughout the whole of the campaign, and were of particular value when the fortunes of war destroyed what had previously been good cribs. Thus after the Allied capture of Tripoli, we waited for a Red/Primrose re-encodement before slogging hard at the latter key. In fact throughout the whole period, great care was taken not to be over-lavish with Primrose, and in March 1943, it was taken over by a "kind of fourth Watch" (later the Cwatch) who examined likely kiss pairings, and this helped to save the work of the main Watch. Dragonfly, a new key of short duration,(Fliegerkorps Mar.Sch.Tunis)was dealt with in the same way.

From April 1943 onwards, with the Allied victory in Tunisia merely a matter of time, a shift in emphasis was already beginning to take place. The final stages of the battle in Africa were on the whole allowed to take care of themselves. The result of this was not only that more time could be devoted to Primrose, but more important, that many non-Mediterranean Air keys could now be dealt with, such as Snowdrop in the West and Hedgehog in the East. Keys like Primrose and Locust were now taking on a more "European" appearance, and the stage was set for the opening of the Italian Campaign.

One final point is worth noting about the cryptographic attack on the African keys. Interception of the messages was largely carried out in the Middle East, and this led to a certain delay in their arrival, and often to a large number of unsatisfactory or undoped texts. Despite this, the collaboration between stations as far afield as Derna or Sarafand and the central organisation here in the Park was an example of effective and efficient co-operation.

Pantellaria

[illegible] there now began to appear a certain [illegible] Red and Locust respectively. The long range [illegible] which had used Red until the beginning of [illegible] to use a key of their own, Squirrel, which, although [illegible] most difficult to deal with on an operational [illegible] on no-encodements from Red and Locust - intrinsically very [illegible] - but it later developed quite a spate of [illegible] of depth. It never was a good crib key. Its new offshoot of Primrose was Mayfly, and after a short spasm of [illegible], it settled down to give us long-lived cribs, Hawthorn III and Hayspruce. Its life as a Watch key was a short one, and it was passed into the hands of the Qwatch and ultimately of Pancake. It never was a specifically Mediterranean key, and its [illegible] with its transport in all parts of the German occupied territories. The offshoot of Locust, Puma, fell into a very different category. At first it dealt with Army-Air co-operation in Sicily, but soon its scope was extended, so that although it temporarily disappeared, it returned to supplant Locust in Italy, and to be one the Five key, of vital importance during the Allied operations further North. Its importance grew while that of Squirrel diminished and most of the Squirrel frequencies either faded out or tried to cover their decline and disappearance by sending inordinate amounts of spoof traffic. Other offshoots of Primrose - Sheep and Lovecat - never provided very profitable recreation.

In November 1943, there was considerable uncertainty about which keys were in use, and what was then thought to be Locust was in fact Puma, while what had been called Squirrel was Locust. From this time onwards Puma usurped the position of Locust as the [illegible] key in Italy. For a time there were valuable exchanges in link to cover the Italian operations, and reinforcements on many occasions from link to Albatross, the key [illegible] key, but also from Liverpool also, and its traffic often [illegible] on [illegible] but was also always [illegible] on [illegible], and many of the other keys [illegible] were only in the minor keys.

[illegible] the Allied landings in Sicily, considerable [illegible] Locust like it which on the Mediterranean keys [illegible] Red to communicate from [illegible] dealing with the [illegible] [illegible] had its [illegible] to [illegible] [illegible] [illegible]

spurt of short messages which were not sent over a long period, but which made early breaking possible. At first these messages were purely routine messages, these were followed by the "Diaries", the routine reports of the liaison officers. Occasionally from this row, [illegible] a report would stand out as a workable crib - [illegible] perhaps the best example of this, a report by the [illegible] Division.

In the meantime, Primrose, now reduced in status to the key of [illegible], sent little of any importance other than the [illegible] Reports, still re-entered into Red, and the method of breaking was still dull and uninspiring, chiefly by tuning messages. When the tuning messages disappeared, breaking became very difficult. Leopard too was very black patches with the disappearance of the J,N,T frequencies, but determination to hold on to it, despite the rival attractions of the new Western Front keys, was repaid when Leopard and Primrose united happily in one key in October 1944.

The Allied advance in Italy, which was far less spectacular than the sweep from Avranches to the Rhine, gave the Italian keys a long and normally unhealthy life. The short reports which marked periods of inactivity were far more valuable to us than the disintegrating operational traffic, sent during our advances. Our best cribs tended to come from behind the front line, Meyer-Bothling sending his reports on partisan activities from the Adriatic coast, or weather experts in Venice sending out reports to Pola. After the fall of Rome, it was very difficult to hold a grip on the keys. The Flivos who had previously sent out their battery of messages day after day, fled with their "Truppe" into the far reaches of the Gothic Line. Although Puma continued to be broken regularly mainly on more standard and general reports and on Recce re-encodements from Red, this initial disintegration was an unwelcome foretaste of the shape of things to come. Technical security methods had already been tried in the Mediterranean (in addition to security devices like rehkeys), the chief of these being the Zusatz Stecker arrangement in the early summer of 1944. In November 1944, a much more serious blow was struck. The Flivos had already sent a wealth of messages ominously describing in detail the distribution of Reflector D. It was felt by the experts in Hut 6 that while the use of this reflector would be annoying, Reflector B would continue in use as well, and we would be able to break the key in the same way that we were breaking Jaguar or Red. However, Puma went over solidly to Reflector D in the middle of November, and the period of regular sustained breaking was at an end.

In any case, there was little doubt in November 1944 that Italy was a subsidiary theatre of operations. The Germans had been pushed back to their own borders, but still held firm in the hills of Italy, ensuring their mastery of the Lombard plains. The Allied armies were not yet ready for the final advance. Most of the attention of the but was rightly concentrated on the Western and German keys, although Puma and Leopard remained on Watch keys, where they still received vigilant attention from their admirers.

1,913. The Balkans

For a year from the autumn of 1942 to the autumn of 1943, Gadfly was treated as a Research key, though in its last stages, it was dealt with by the Watch. Messages from the Middle East arrived late, and back days were blisted; texts were often poor; cryptographically, chiefly because of lack of bombe time, the key was

often neglected. This particularly applies to the period from October 1942 to July 1943, when only re-encodements were tried, and they were only exploited sporadically, mainly by visitors. Greater attention was given to the key after the end of the African Campaign, and the results were immediately plain. In August 1943, a complete month's breaks was obtained. On October 1st, it became a Watch key on account of its increased intelligence importance and urgency. It was no longer the key of Fliegerkorps X, but of Luftwaffenkommando West. In the Watch, it received careful and sympathetic attention, and enjoyed a great run of success. It was always difficult and often tantalising, for cribs came and went in a bewildering manner, and even those that stayed saw frequent changes in their form. Thus an Auffüllungsbefehl became an Einsatzbefehl overnight, as in the case of Konsulat Rollfeldmeldung Bandenlage, and Ju-Ab were the chief standbys, and though the intelligence value of such messages was not urgently important, the accumulated information given by Gadfly as a whole presented a fairly clear and often interesting picture of the complex Balkan situation, and would have been of vital importance if the forgotten Balkans had been the scene of a Third Front.

In the prime Gadfly produced two strange and unusual [illegible] The chief of these, Yak, read the key of Fliegerführer Ukraine, and although it used Hand book cribs and G.A.F. habits of procedure it was also quite unlike Stecker, crashing and non-Fliegerkorps usual [illegible] and record runs of the same reports as Weymouth, the Balkan Air Force Intercept station showed the successful treatment of this key, which was the most puzzling dealt with on Research lines, though it had a sharp spell in the Watch. In the dim days of early 1944, with the Axis armies and much portions attacking the last unconquerable [illegible] the Balkans, Yak was, if anything, of more value than in any subsequent period.

The second offspring of Gadfly, Ellida, was even more short-lived, for it did not survive. At the end of January 1944, the Mediterranean Traffic did not decode on the Gadfly key. The traffic of one of the keys was broken on a re-encodement and revealed [illegible] self-stecker; a further day produced sixteen self-stecker. [illegible] appeared on the beginning of September, but before it was, it had the latest look of glory. When it seemed likely [illegible] thought [illegible] there would be a great extension [illegible] Party Duty at Red, it was thought that 'Rotten Luck' [illegible] application of keys to the general key might well save us any [illegible] suspects in the Balkans were fully strongholds of Reference [illegible] Duty at Red, such re-encodements were never necessary, and [illegible] Ellida, with its disappearance, a Research Key - [illegible] Gadfly, even was given a specially high breaking priority.

[illegible] Gadfly itself in quite a long story. [illegible] Balkans was hardly responsible for the system [illegible] of the Balkans was [illegible] [illegible] [illegible]

islands, several keys were in use. Although by the end of the year the position had been cleared up again, many different Gadfly keys- in hatted order, reserve keys etc. - were in use during the interim period, and created a terrible mess both for the cryptographers and the traffic analysts. The growth of a Central European complex during this period is also very noticeable and is dealt with elsewhere.[1] It had often been wondered what would be the effect of the impact of keys like Orchid and Ermine on the Balkan set-up after the Russian advances beyond their own frontiers. As early as June 1944 there was a re-encodement from Gadfly to Orchid that broke the Orchid day. As the year went by, Gorilla (the key of Luftflotte 4) came more into the centre of the cryptographic picture, which was further complicated by the arrival of Fliegerkorps II(Locust) in the same area. Gadfly began to play a varied but on the whole diminishing role. Thirty two breaks were secured during 1945. Yak had ten breaks at very heavy bombe cost. The interest in the Central European keys grew, however, and reached its height during the last weeks of the war.

1.8035 The Last Months

In addition to the last remnants of the Balkan keys, Leopard and Puma continued to be broken in 1945. The breaking of Puma was an important technical problem. The first thing necessary was to find a suitably long re-encodement from Red(there were re-encodements from Leopard also but they were not suitable)and then to prepare it for the D-breaking machinery. Seven Ds were broken in this way on Giant and Duenna. A break on a Puma D period in January revealed that the traffic was not only on Reflecter D, but almost solidly on Enigma Uhr as well. Although one other D-break was achieved,it was impossible to follow up the breaks and to secure the remaining days of the period. Previously these had come out quickly on the short weather cribs. Now these cribs had either disappeared or were too short to use for Enigma Uhr menus. From the end of February onwards, Puma had virtually to be written off, and even the Recce re-encodements from Red almost dried up.

Leopard too had its Reflector D, but the Flak units, which passed most of the traffic on the key continued to use B. Consequently we were able to break the Ds by cribs, bobberies and occasionally skirts, without a great many gaps, though often with a good deal of difficulty. Fourteen Leopard Ds were broken in all. Apart from the problem of D, Leopard had an extremely good run in 1945. The number and strength of the cribs was greater than ever before, and in March for instance only 4 Leopard days were missing. A comparison of Leopard and Puma breaks and bombe hours during 1945 is of considerable interest:

	Leopard			Puma		
	Breaks	Time	Hrs/Bk	Breaks	Time	Hrs/Bk
Jan. 1 - Jan. 27 :	23	1268	55	15	925	61
Jan. 27 - Feb. 25 :	22	1765	80	7	756	108
Feb. 25 - March 31:	31	1630	53	2	1742	871

This shows that in the last period, more time was spent trying to break Puma than was spent securing the thirty-one breaks on Leopard. Probably even more Leopard breaks would have been secured had it not been for bad interception. Leopard was the last of the keys to have almost all its traffic intercepted in the Mediterranean, and it never received very high priority from the Italian intercepting

1. See the separate account of the Eastern Front and German Air Keys.

stations, who had the Italian Army keys as their first commitment, and who could not spare more sets on the M/F band. Leopard too in the last stages of the war became bound up with the Central European keys, and re-encodements to Gerilla and similar keys began to appear. The German armies which had once been supreme from Alamein to Sicily, and held Athens, Belgrade, Rome and Tripoli were now squeezed into a small pocket, all that was left of the mastery of the Mediterranean. It was with the small pocket that the last work of the Watch was concerned.

1. 804 THE AFRICAN ARMY KEYS

1. 8040 General

It is stressed throughout this history that the German Army keys were usually spasmodic in appearance and intractable to deal with because the Army signals officers were schooled to construct landlines and to send as little by wireless as they could. In Africa, however, the vast distances and difficult country made intercommunication by wireless essential, while all traffic home to the mainland had to go over the air. And up to the last month of the campaign, when a Fish link to Tunis was constructed, the entire traffic had to pass in Enigma. Here then was Hut 6's chance to bring off its most spectacular coup. The prize was detailed information about the strength, disposition and intentions of every unit in the field, sidelights on the mind and character of the commanders, and glimpses of the attitude of the authorities in Berlin to their C-in-C in Africa. The Chaffinches were not all broken all the time; for periods of months none of them came out at all. But the measure of success will be judged by the volume and detail of intelligence which flowed from Hut 6 via Hut 3 to Cairo and Algiers from early in 1942 to the end of the battle in May 1943. It is surely inconceivable that any campaign had ever been conducted before with such advantages as Hut 6 was able to afford to our commanders in that period.

For those engaged in the work it was a most fascinating and exciting struggle, with the odds, as always with Army keys, fairly heavily against the cryptographer. At no time was one so closely in touch with the course of the battles as when the daily report of Rommel's Army provided not merely an excellent crib but also a first-rate off-the-record story.

1. 8041 The First Breaks: 1941-2

The breaking of the African keys fell into two distinct periods, September - November 1941, and April 1942 - May 1943. Heavy traffic soon appeared in Africa following the arrival of the Germans there early in 1941; the key used, which was then known as A.F.5, was broken once in March and once in April on cillies without, however, showing up any cribs. One or two breaks in September were more profitable, and until mid-November there was an average of at least one Chaffinch break every two days. Of a variety of cribs the best were two day reports, one of them being the famous Bison, the Rommel Tagesmeldung which usually began AN (X) IDA BISON (X) UEBER (X) IDA PINTSCHER; Ida Bison and Ida Pintscher being the code names for the operational staffs in Berlin and Rome.

The British offensive in November had two immediate repercussions in Hut 6. First the Army captured and sent home the Chaffinch I and II and Phoenix keys, together with their reserve keys, which enabled us to decode the complete Chaffinch traffic for the month up to November 23rd, when the Germans brought new keys into force; and also to study for the first time the rules of Army keys. At this time they were obeying the non-clashing rule, which was of great importance to us in days of few bombes; and also the "Army ringstellung rule" which could occasionally be of help, especially when there were cillies.

Secondly, the offensive was so disturbing to all the German elements that they ceased to send any cribs, and the Chaffinch simply ceased to be broken through the period of the advance to Benghasi and retirement to Gazala.

In March hope of Chaffinch breaks revived with the appearance on Gadfly on many days of what was clearly the old day report of the Panzerarmee, and Sixta were able to point out that a routine R.E. between two of the Chaffinch keys was almost certainly the same thing. It was now clear that there were three Chaffinch keys in use - Chaffinch I and III which were general keys possessed by all the main supply bases in Africa and also by Italy and Salonika, and Chaffinch II which was a special key for communication between Rome and the operational H.Q. in Africa (Sondermaschinenschüssel Rom - Panzerarmee Afrika). Phoenix (Maschinenschlüssel Panzerarmee Afrika) was used for operational communications between Division and Corps, Corps and Army in Africa.

1. 8Q42 The Re-entry into Chaffinch, April 1942

The routine re-encodements between Gadfly and Chaffinch were dealt with currently failed and two members of the Crib Room were therefore detailed to make a thorough investigation of the Chaffinch problem. It appeared that the message on Gadfly was routed from the Panzerarmee to Fliegerführer Afrika, while on the Army networks it went from Africa to Rome on Chaffinch II and Rome to Salonika on Chaffinch III, or sometimes Chaffinch I. Thus, whenever a Gadfly version appeared, one had the alternatives of attempting the R.E. into either Chaffinch II or Chaffinch III, and several days of both keys were tried without success. One day a very short report appeared saying simply WEGEN SANDSTURMES AUF PANZERFRONT KEINE AENDERUNG DER LAGE.

This, together with the usual address and signature and designation as the Tagesmeldung of the 17th April, made up the whole message. And with the German checked by the linguists as correct and almost certainly invariable, the crib experts proceeded to stagger the stretch through the Chaffinch versions and run all the possible positions, which were few in number; but they failed. The message was then attacked by statistical methods, for a "boil" had revealed that while the Chaffinch II versions (the Bison) were certainly not in their old form, the Chaffinch III transmission had far fewer than the number of crashes expected by random on the beginner TAGESMELDUNG (Day) X (Month) or VOM (Day) X Month. These forms were therefore run and the day came out. It then appeared that the text of the R.E. had been run in the correct position, but unfortunately no one had noticed that PANZERFRONT (the Tank Front) was a rather odd expression; it was of course corrupt for GANZER FRONT (the whole front), and the single wrong letter in the crib was sufficient to fail the short, an interesting example both of the luck of the game and the letter perfection which Hut 6 had to achieve.

Rapid exploitation of this break enabled Chaffinch to become a full operational commitment very soon afterwards, and until the end of August the general position remained substantially the same. There was the one crib on Chaffinch I or III, known as the Panzermeldung, and the same crib in its previous transmission known as the Bison on Chaffinch II. Apart from this message,

there was for a month or so a strong alternative in the crib Marinebericht on Chaffinch III, and there were one or two weak cribs which were just good enough to break a day or two before they disappeared. In addition, occasional unexpected successes were achieved by methods such as cillies or reading in depth which, while valuable, did not alter the general outlook of the keys.

1. 8043 April - October : Improvement in Technique and Increasing Success

For three or four months, then, the breaking of Chaffinch proceeded by much the same methods, and with much the same amount of success. At this time very little Chaffinch I was broken - it was the smallest key and we had not discovered the reason for its existence. Of the remainder, normally eight or nine out of a possible fourteen keys were broken each week, with double figures occasionally when things went well, and as few as four in harder times.

In this period every success represented hours of toil by members of the Crib Room; every break was hailed with delight by those on duty; and the incoming shift could usually tell from a glance at the faces of their predecessors whether their fortunes had prospered. There were three factors which precluded us at this time from achieving the completeness of success which we were enjoying on the Air keys: (1) the small number of bombes, (2) the poor quality of Chaffinch cribs, and (3) our own inexperience in dealing with Army keys. The first and second of these were, of course, closely interconnected, for with so few bombes nothing could be run unless it stood a fairly good chance of being right; the Chaffinches depended on one crib, which said on its good days TAGESMELDUNG (Day) X (Month). It was known sometimes to vary this with TAGESMELD X (Day) X (Month) or TAGESMELDUNG VOM (Day) X (Month), and normally these three forms were run. By the time they had failed the next day's message had come in and it was time to start running the same forms all over again. We knew that sometimes it had the signature(VON PANZ X ACK X ACK X AFRIKA) at the beginning and that sometimes it used forms like GEHEIM X YY TAGESMELDUNG, etc. But there simply was not bombe time to run them. There can be no doubt that another twenty or thirty bombes in this period would have enabled us to come very near to completeness. The other factor which perhaps cost us several days which we might have broken even without more bombes was the novelty of the problem of re-encodement. Before the Chaffinch era keys had been broken on R.E.'s, but with good cribs on most Air keys, one did not usually use an R.E. unless it produced a relatively simple and certain answer. Now every success with the Chaffinch Panzermeldung meant at least one R.E. into the Chaffinch II, and this was a key without any other crib. It was now that we perfected the technique of selecting the ideal stagger stretch, of finding the toil-breaks, and of analysing the alterations in a routine R.E. It was to improve our tally on these messages that the card system was adopted whereby the different versions of the decoded R.E.'s - Chaffinch II and III and Red or Scorpion II if they happened to appear in Air traffic - could be compared at a glance. Thus one saw the standard lengths of the addresses and signatures in the different versions and allowed for them; noted common differences in abbreviation and punctuation; and in many ways obtained an insight into the differing outlooks of the various German encoders. Perhaps the

best indication of the improvement in our methods is shown by the fact that in the first four days of August the Panzermeldung suddenly appeared three times in Scorpion II, giving re-encodements into Chaffinch II and III each day. In spite of hours of work by all members of the Room, only one out of six possible keys was broken. Whereas when we had a return of the Scorpion version at the end of September no days at all were missed for over a week.

Throughout September and October increasing bombe power and improved technique of cribbery brought us much closer to the goal of twenty-one Chaffinch keys a week. By this time there were enough machines to allow more expensive methods; for analysis revealed that messages with certain routeings tended to start in the same way, e.g. Mersa Matruh from Tripoli:

AN X KARPFEN X VON X UNGEHEUR,

Karpfen and Ungeheur being two of the code names of which the Army in Africa was so fond. And such beginners were as good on Chaffinch I as on III, for we had by now discovered the Army use of Staff and ordinary keys. Chaffinch I was O.K.H.Stabsmaschinen-schlüssel Nummer 1, and Chaffinch III the corresponding O.K.H. Maschinenschlüssel, and all Geheimekommandosache traffic was sent in I while the rest came in III. This was well worth knowing because it meant that one could recognise the grade of traffic from the outside. When, for example, the Chaffinch Panzermeldung was sent in Chaffinch I, we knew that it could begin with the Gkdos but not the Geheim forms. This was simply one example of the tightening grip which we were obtaining over these keys and the success obtained inevitably led to German doubts as to their cipher security. One enquiry produced the decision that "the Enigma was safe as long as the wheelorder was changed three times" (this measure was generally introduced in the Army in July 1942). And a later order said that addresses were to be buried and nonsense words used in front of standard beginnings; and within a week or two wahlworts were in general use. This measure was a crippling blow to Hut 6 at the time with its extremely limited bombe-power; but two circumstances enabled us to proceed for two or three months with success not appreciably less than before. Of these the more important was the growing tendency for re-encodement between Chaffinch and Phoenix which hitherto had been quite unconnected with the other Army keys.

1. 8044 Phoenix: the Difficulties of Overseas Interception

The forward Army units naturally required low-power short-distance wireless transmission, and as a result the medium and low frequencies used were normally inaudible in this country. Interception in Africa, while not up to the superlative W.O.Y.G. standard, should have been sufficient for Hut 6 requirements and in spite of errors in morse, teleprinting and typexing, it was usually possible to attack the traffic - when it arrived. The typex situation in Cairo, over which Hut 6 had little control, was the weakest link in the whole Enigma organisation at this time; it is quite clear that with better arrangements for sending the traffic home Phoenix would have been broken at an earlier date and thereafter much more often and more quickly. Furthermore, the anomalous situation would not have arisen whereby we were able to break the key currently on a crib and unable to decode most of the traffic for very many hours because it had not arrived.

Phoenix was not actually broken until June 1, 1942, although several good cilli menus had failed through interception before that time. Other days were broken on cillies but no crib appeared except for a brief period of two or three days, when one unit suddenly began to announce "No change" every two hours, and a day was broken on NICHTS NEUES X GIERLING X, the complete message. Many of the days broken came out very late because of the accumulation of traffic over a period of days, which meant that a message vital to a cilli menu might be one of the last to arrive. Much clever hand breaking was done too with the aid of ringstellung tips and the operation of the block rule; but it was not till near the end of August that any attempt could be made to deal with the traffic operationally, when the cilli breaks at last revealed some cribs. These were very short morning messages reporting quiet nights, e.g. NACHTVERLAUF RUHIG
or NACHT RUHIG VERLAUFEN

which had the virtues of certainty and early appearance, but were sometimes too short for running as anything but single menus risking a number of turnovers. This, it must be remembered, was before the days of hoppity bombes; and various ways therefore had to be found to account for the days when the turnover came in the middle of the message. Ringstellung tips enabled hoppities to be run and it was presently noticed that the cribs tended to have nearness indicators which enabled turnover assumptions to be made. With cillies reducing the wheelorder on many days, breaking went on through September with scarcely any missing days. And early cribs coupled with a speedier return of at least a part of the traffic meant that the intelligence could be used operationally. October was an even better month than September and then Alamein and the advance brought floods of traffic but the demise of all the cribs.

1. 8045 The Wahlwort Era: the Phoenix-Finch Complex: December 1942-April 1943

By great good fortune however the Panzermeldung and Feindverhalten (Rommel's 1A and 1C reports) began to appear on Phoenix in transmissions to Superlibia, i.e. the Italian High Command. This enabled us to break one or two November and December days by R.E.'s and keep in touch, and then at the end of December the remains of the Afrika Korps settled down to hold a line and all the old cribs returned.

Meanwhile the introduction of nonsense-words as an anti-crib measure had been ordered in a Chaffinch message at the beginning of December and after a brief period in which the German operators, misunderstanding their instructions, made things easier for us instead of more difficult, the entire Finch groups settled down to the new procedure. Whereas one formerly used a crib at the beginning of a message, one now had to allow for a nonsense word of from four to fourteen letters long, and thus the crib(on the more unfavourable days) would have to be run in as many as ten times the number of versions. Further, breaking on straight addresses was now out of the question; for whereas a favourable address might have as few as three alternative forms of which one could eliminate one or perhaps two by selecting a message on which they crashed, under the new regime one would have to stagger all three forms over a range of ten, and would find at least twenty possible versions.

With the bombe-power then available this innovation ought, on reasonable calculations, to have stopped us from breaking the Finches at all except by sheer luck in say, guessing the right position in ten, or by concentrating on perhaps one day a week. However, the rebirth of the Phoenix after the fires of Alamein was Hut 6's saving dispensation. The NachtRuhig crib returned and was sometimes intercepted in this country; while the shift in the scene of the fighting enabled W.O.Y.G.regularly to intercept the Phoenix version of the Panzermeldung, which was also a good crib. It was even now very difficult to hear, and W.O.Y.G., informed of the vital importance of the message, and in particular of its first groups, put a battery of sets and ace operators on to it. Mr.Walton, supervisor of the W.O.Y.G.set rooms, used to take a version himself and there was one famous occasion when the station rang to say that they had just taken ten copies of the message, of which eight had E for the fourth letter and two I; but as Mr.Walton's text was one of the two giving I, I was certainly correct. It was.

With Phoenix broken, it was possible to proceed by re-encodement into the Finches. The Bison had now developed another leg in its journeys, for it was sent from Rome to Tunis in the new Tunis key, Bullfinch. Bullfinch was first broken in November, when the 21st came out on a re-encodement from Chaffinch. Crib Room Research (or C.R.2) at this period made a comparison of times of origin of all Army traffic; and the break of Bullfinch was its first success. Other days were then broken by the current watch on more R.E.'s, chiefly of the Lagebericht West, a general intelligence report sent from Rome to both the Afrika Korps and the Army in Tunis. The L.B.W. R.E.'s as they were called, were some of the most difficult which had to be faced, for the two versions were often widely different in content; that going to Tunis had a section about Rommel's Army which was omitted from the other because he already possessed the information; and vice versa. The method therefore was to find the part common to both messages: a process difficult enough, but increasingly so when the Germans produced what could only be construed as an anti-re-encodement measure, the placing of wahlworts at the beginning and end of every teil. This virtually eliminated the teil-break as a factor in solving R.E.'s; and from our point of view the only good thing about the new rule was that it was not always kept.

The first Bullfinch days, broken at the end of November, were extremely valuable later when the key was used again next month, and with these days together with others broken on R.E.'s from Phoenix it became possible to estimate the full effect of the use of wahlworts. It was clear that they were universally used on everything except Phoenix on which they were rare and only on frequencies of no crib value. Occasionally some of the routine Finch messages were sent without wahlworts by the Rome station, which encoded both versions of the L.B.W. and also the Panzermeldung. Hence it became policy to run these cribs in the first position only each day, giving an average of about one break per week. Meanwhile it was reasonable to expect at least five - and with luck all seven - Phoenix days out fairly quickly each week, with the Panzermeldung R.E. to take us thence into the Finches. So then with Phoenix as a jumping-off ground, most of the vital Finch traffic was broken in January, although reliance on chains of R.E.'s meant that the last link was apt to be reached only after the lapse of some days. The score sheet of the African

keys for a typical week at the end of January 1943 is appended to this report. It will be noted that Phoenix provides the initial entry on six out of seven days while three of the Chaffinch II's were some days late in coming out.

At the beginning of February the Italian Command, Superlibia, was dissolved, and the Rommel reports were no longer sent on Phoenix, with the result that Finch-breaking became dependent on the rare stray R.E.'s from Phoenix or on long stagger jobs on poor cribs like the L.B.W., Lagost or Panzermeldung. However, Rommel's counter-attack against the Americans at Gafsa caused the division of his forces into the Gafsa force, under his own command, and the Mareth force under the Italian, Messe; and both groups from 21st of February began sending day reports which were re-encoded into the Finches. Thus for over a week there was a glorious revival in Army breaking, but from the Hut 6 point of view it was the last bright spell of the African campaign. March and April found even Phoenix very difficult, and there were practically no Phoenix - Finch R.E.'s. At the beginning of April long stagger jobs on the Finches were abandoned as too expensive and unprofitable; under strong pressure from the Intelligence authorities, who even with the net drawn tight round the Army in Tunis, thought the information still vital, they were resumed in the last half of the month and two breaks were quickly obtained; thereafter none. In the last week of April five Bisons and three Lagosts were run in a total of 73 versions without a single day coming out. One more break of Chaffinch and thence of Bullfinch was obtained on a R.E. from Fish on May 9th, and thus the battle against the African Army keys ended, quietly. The enemy's security campaign had caught up with us before the end of the fighting; but by this time the issue was no longer in doubt.

1. 8046 Thrush (Sonder M/S Rom-Malmes) and Other Keys

One or two other keys should perhaps be mentioned in this section although they were of no real significance to the general breaking procedure. Thrush was a special key used for triangular communication between Rome, Greece and Crete, dealing in particular with supplies for the island. It lasted from July to November, 1942, and was interesting to break although with bombe-time scarce it was frequently neglected in favour of more urgent and important commitments. The first break was obtained by R.E.from Chaffinch on July 23rd, and revealed that the operator in Crete used almost invariably indicators of the nearness type, (1, 1, 2) on from the outside indicator. Subsequent breaks on indicators and other R.E.'s showed two cribs Hornschaft and Ankunft, both long supply returns, Ankunft being a statement of the material which had arrived in Crete by air during the day. Further evidence of these messages revealed a three-day cycle which enabled the forms of both the cribs and the indicators to be predicted with accuracy and it became policy to break a day or so per week and otherwise only to attempt to get the day out if there was a R.E.to Chaffinch. For such R.E.'s occurred from time to time, chiefly owing to the location of units of the 164th Light Division in both Crete and Africa, intercommunication taking place via Rome.

Thrush finally disappeared at the end of November, leaving some unsolved problems which probably did not receive the attention they required owing to pressure of current work. On all the latest days broken only part of the traffic decoded; on one of them one or two messages came out on an illegal permutation of the

wheelorder but the remainder were still dud. And still we don't know why.

The Army in Tunis, Panzer A.O.K.5, produced its own key, analogous to Phoenix, which was named Dodo in view of its approaching extinction, and broken two or three times on cillies. No crib and no more cillies came before the final surrender. And hence further breaks had to await the creation of a new and equally ill-fated 5th Panzerarmee - and hence a new Dodo - during the final Western campaign.

Falcon I and Falcon II (then known as Merlin) were each broken a few times by R.E.'s from the African Army keys, owing to the variety of keys which appeared on the wireless link between Rome and Salonika. This rather happy-go-lucky state of affairs puzzled us for a long time: but it is clear now that the reason for the presence of the Falcons on the link was to enable messages to be forwarded without re-encodement on the wireless - more usually the teleprinter - link between Salonika and Athens. For Athens did not possess the Chaffinch keys, but only the Eastern O.K.H. and the general keys, Vulture and the Falcons and Mallards. Such inter-area connections were of great cryptographic significance for thus light was brought to the lands of darkness, but in this instance they were of more importance from the point of view of the Balkan and European keys than of the African group and hence will be considered in a separate section.

1·8047 Appendix

C.R.1 WEEKLY REPORT

Week Ending 30th January, 1943

Date	CHAFFINCH I	CHAFFINCH II	CHAFFINCH III	BULLFINCH	PHOENIX
Jan.23		Lagebericht West R.E.	Panz	Bison R.E.	Morgenmeldung
" 24		(R.E. from Phoenix)	Panz R.E.	Bison R.E.	Phans
" 25	Panz R.E.	Lagebericht West		Lagebericht West R.E.	1545 Nacht Ruhig
" 26	Panz R.E.			Bison R.E.	1545 Nach Ruhig
" 27	Panz R.E.	(Lagebericht West)		Bison R.E.	Phans
" 28	R.E. from Bullfinch	(Lagebericht West) R.E.	Panz R.E.	Morgenmeldung R.E.	Morgenmeldung
" 29			(Panz R.E.)	(Bison R.E.)	(Morgenmeldung)

BRACKETS indicate breaks since midnight 29 - 30 January, 1943.

215

1·805 THE ITALIAN ARMY KEYS

1·8050 General

The campaign in Sicily and Italy with its long periods of static warfare and consequent facilities for landline communication offered Hut 6 but poor material for exploitation in comparison with the fight along the southern shores of the Mediterranean. Traffic came sometimes in floods and sometimes not at all; but most commonly in trickles, wireless links being kept open in case of need and used as an overflow for the teleprinters. Brief spells of heavy traffic sometimes led to breaks which could not be followed up because the flow dried up as suddenly as it had begun. For the cryptographer this was dispiriting; for Hut 3 it meant that intelligence from Italian Army keys tended to be fragmentary and mostly of a low grade. Fortunately the Fish section was able to fill the breach by continuous and complete breaking of Bream; so that it was left for Hut 6 to act on the assumption that "What is worth encoding on the Enigma is worth decoding", and do what it could with anything that came to hand. The result was normally a grey picture of difficult breaking and low-grade intelligence, brightened occasionally by spectacular flashes of brilliant success and priceless information.

1·8051 Before the Surrender of Italy, May - September 1943

The Italian campaign from the Hut 6 point of view began some time before the landings in Sicily. With rapid movement of German troops into Italy and the islands during May 1943, following the surrender in Tunisia, new keys at once appeared, Albatross I and II, which were later identified as the key and staff key of the 10th Army, and Cormorant, a special cipher used for communication between Rome and one of the German units in Sardinia. These keys were examined by the newly-formed Army Research Section, and a Cormorant break on a R.E. from Primrose was one of its first successes. This key was broken once or twice afterwards on R.E.'s from Albatross but never showed any sign of producing any cribs or cillies, and, with wahlworts used on all messages, was normally quite unbreakable. It finally disappeared with the evacuation of Sardinia.

Albatross I, with an average of 150 messages a day at the end of June and the beginning of July, was obviously of the first urgency and importance with the invasion of Sicily drawing near. By good fortune cillies appeared from a station in Sardinia and a number of days were broken, disclosing no crib but an interesting stecker pattern in the July days whereby the pairings were at a fixed distance each day, the distance going up one a day. Thus on day 1, the stecker would be three apart (e.g. A/D, B/E, C/F, etc.) and on day 2, four apart (A/E, B/F, D/G). With this assistance it was possible to break nearly all the July days on short cribs or in many cases on cillies by hand. The invasion of Sicily was followed a few days later by the transference of Albatross from the Research Section to the Watch. For it was seen that breaking could be attempted currently while the stecker rule was in operation, and it was hoped that in due course cribs would rake their appearance. Albatross II was occasionally broken in this period too, but entirely by re-encodement. Nile (Med.Naval), Locust, and Cormorant all gave R.E.'s, but none of them revealed a crib.

The turn of the month brought the end of the stecker patterns and breaking in August depended on the occasional bursts of cillies and such cribs as had appeared during July. Of these the only one

of any value was a Tagesmeldung from Sardinia, and that was probably the most unreliable crib ever regularly to be run on any key. And yet it broke several days, including one when the form written out was entirely wrong but happened to be made into menus of which one had letters in common with the actual text ! Presently another and better crib appeared, a report on mine-laying; and later a really good crib dealing with the oil supply in the Islands. One way or another three or four days were broken each week until the surrender of the Italians at the beginning of September; whereupon the islands were evacuated and two of the cribs disappeared. From now on for many months Albatross I was broken only very occasionally on cillies or R.E.'s from Bream; the cillies came from a unit which used the trigram ENG as both a fixed call-sign and the indicator of many of its messages.

1.8052 Surrender of Italy and Rise of Shrike and Bullfinch: September 1943 - February 1944

The impending Italian collapse near the end of August caused the German High Command to send large forces through the Brenner; and Heeresgruppe B, the staff of which had been moved from the Russian Front, established itself in Munich to take charge of the new divisions. Its arrival was immediately reflected in the W/T picture, and a short morning message which soon appeared rapidly presented us with our first break of the new key, Shrike I, on the guessed beginner MORGENMELDUNG (VOM) (Day) X (Month).

After an initial spurt of breaks in the course of which most days at the end of August and the beginning of September succumbed, and the key was transferred from the Research Section to the Watch, there was a long blank period when the crib was not heard. However, after a gap of three weeks it came back, and thereafter one crib appeared as its predecessor vanished so that four or five days a week were broken steadily until the traffic finally petered out in February 1944. Shrike, although originally used by Heeresgruppe B and all its subordinates, was almost certainly the key of the army in the north, A.O.K.14. When A.O.K.14 moved south it left part of its forces, together with its key, behind, the northern portion being named after its commander "Armeegruppe von Zangen". Hence, there was later a new key of A.O.K.14, which was named Kingfisher.

Shrike was an interesting key to break and the decodes made good reading. It was fortunate that wahlworts were not commonly used on this key, and very rarely on the crib messages. Thus Hut 6 was able to provide a fairly complete intelligence picture of the Italian front for a spell of over a month at the beginning of 1944. For while Shrike dealt with the forces in the north, a key had been discovered and broken which adequately covered the fighting front in the south. A very long daily routine message was observed in November and December passing from a station in Italy, thought to be A.O.K.10, to O.K.H., and after speculative shots based on the evidence of crash analyses had failed, a stagger of the date EINS FUENF X EINS ZWO was sent on the message for December 15th to be run on the Washington bombes. This succeeded early in January, the message proving to be the Tagesmeldung of A.O.K.10. In spite of the use of wahlworts, the message was a good crib on the stretch TAGESMELDUNG (VOM) (Date) X (Month), which had to be staggered over a short range at the beginning. On most days too there was also a Morgenmeldung, and sometimes a Zwischenmeldung, so that once the original break had been achieved nearly every day came out until the disappearance of the group early in February. This was traffic at the highest level of urgency and importance, and its similarity in these respects

to the Bullfinch of the Tunisian campaign - the two keys had nothing else in common - led to the second use of the name.

Bullfinch and Shrike were the cases in the desert of the Italian Army keys. They were regularly breakable over a period and in intelligence content they compared with the Chaffinches of Africa and the Puffins and Bantams of the days to come in the West.

1.8053 Kingfisher: May - August 1944

From the end of January to early in May 1944, traffic from the Italian front was at its lowest ebb. Then there was a marked increase, and several keys appeared of which one began to come out regularly for the first time. This was Kingfisher, the key of A.O.K.14, which was now at the front although the traffic was of supply rather than operational content. It was broken for several days on R.E.'s from the associated Playfair, and then on cribs. In spite of some blank patches a certain amount of Kingfisher was broken from this time forward until the end of August. Breaking was mainly dependent on cribs sent by the 26th Panzer Division, which withdrew from the line in August and reappeared a few months later under A.O.K.10. The cribs were thus transferred from Kingfisher to Albatross, and they were of sufficient reliability to ensure fairly regular breaking. The best of them was a message signed by a certain Hauptmann Krupinski dealing with available storage space (Freier Nutzraum); perhaps the Hauptmann did his own encoding; or maybe it is that a man can be a hero to his own cipher clerk. At any rate the indicator of the message was always part of the name Krupinski. At first it was always KRU, but later for variety's sake, I suppose, our friend indulged in obscurer portions, used either forwards or backwards, such as PIN, SKI, RUP, PUR, and even KSN. While the indicator remained KRU, it was possible to run a shorter crib with the assistance of the three extra constations and known turnover; but afterwards it was only of assistance in finding the ringstellung.

1.8054 Revival of Albatross: October 1944 - April 1945

In August Kingfisher breaks became rare and finally stopped altogether. Meanwhile a break had been made into Albatross by re-encodement from Sparrow, and more than a week's steady breaking achieved on a crib; but then the crib died, and Albatross was lost again. But better things were to come. During September Mediterranean traffic rose in volume, and early in October routine R.E.'s of reconnaissance reports between Puma and Albatross were spotted by Sixta; and success with some of these revealed good cribs which enabled breaking to proceed until the Allied break-through in the final offensive in April. In this final phase traffic was steadily rising in volume and in intelligence value during the last two months. Before that time it dealt with very minor matters and the content was rated very low. Yet - this happened with many keys - there were anxious enquiries from Hut 3 whenever Albatross failed to come out for a few days ! Actually in this last period of about six months there were few big gaps, the only notable one being about Christmas, when all the old cribs disappeared and the great power of a message which had just been intercepted for the first time had not been realised. This was a crib of almost invariable form for about eighty letters, and for many weeks it made the breaking of Albatross purely a matter of routine.

1·8055 The Puffins

Albatross and Kingfisher were keys designed for use by A.O.K.10 and A.O.K.14 and their subordinates. At the higher level, Army - Heeresgruppe - O.K.H., there was normally very little traffic in the Italian theatre. However, the W/T links were there if required, and when they were used the keys were obviously well worth breaking. At this level the keys used were most commonly Puffin I and II (originally called Jay and Puffin) and sometimes the Armee keys of the Army involved, or its staff equivalent. There were spells when Albatross II or Puffin II were broken on the IA and IC reports of O.B. Südwest, known from their contents as the "Limbo" (Lage im Bereich O.B.S.W.) and the Feindverhalten. Unfortunately they were poor cribs and very expensive to use, so that most of the breaks made on them were by re-encodement; for this pair sometimes appeared in the Air keys, Red or Pink, and frequently on Fish. After D Day the Puffins were used in the West as well as in Italy, and in fact the first two Western Army messages decoded were on Puffin II of June 7th, which was broken on one of the few cribs which ever appeared on this key, the Hunter. This was a Y intelligence report on Tito's activities, sent from Heeresgruppe F in the Balkans to Heeresgruppe C in Italy, and it ended with a serial number which could sometimes be predicted. But as Western traffic increased, the Puffins from the breaking point of view, became entirely Western keys: Italian traffic was decoded on them, but it had little crib value. Even so the veterans Feindverhalten and "Obswag" (descendant of the Limbo) are recorded as each scoring once on Barnyard keys of August 1944, thus possibly giving us some consolation for their previous shortcomings.

Normally, then, there was very little high-level traffic from Italy, and when it appeared it was expensive and disheartening to break.

1·8056 Sparrow

One other Army key was in general use in Italy, that used for communication between Y-intercept stations. It was broken first on cillies in April 1943 and subsequently on cillies and cribs. In the early months the cribs tended to be short-lived, and continuity was with difficulty maintained on spasmodic outbursts of pronounceable cillying, such as the sequence which a thirsty operator produced in April 1943, VIN, GIN, COG NAC, WAS SER. But in September the two-hourly D/F reports, which earlier had been used as cribs, returned in a new form and made Sparrow-breaking a simple matter for a long time afterwards. The messages began with the times during which the bearings were taken, e.g. VON JJJJCCJJ BIS JJBBCCJJ, i.e. von 0030 bis 0230, the letters A-J being used for the figures 1 — 0. This crib was called "J" for obvious reasons, and while it lasted Sparrow was dealt with in the Watch as an operational key. This was partly because it sometimes produced an urgent message, and partly because there were very occasionally R.E.'s into Albatross.

The "J's" were liable to disappear from time to time and in February 1944 an alternative crib, a long report about the Allied Order of Battle was successfully used for the first time. It began FULA (Date), Fula being an abbreviation for Funklage-meldung, and was easily recognisable by the great length of each teil - often 400 - 500 letters. "J" with support from Fula broke a very large number of days until July 1944, when both finally

vanished. Re-entry was made in November by running the beginnings of messages of a known type in a very large number of versions. These were Allied low-grade reports, decoded and translated, which either began with the time of origin of the Allied message or in one of several common forms, e.g. EINSFUENF (X) FUENFVIER (X) UHR, BOMBARDIERUNGSAUFTRAG, FDLK AUFKLX MELDET, etc. By choosing a message which rejected well one or two days were broken without undue expenditure of bombe hours, and it was then seen that the old Fula was still present under a new name, Nalm, which stands for Nachrichtenaufklärungslagemeldung or "Y-situation report". There were two versions of this, one on the general key, Sparrow II, while the other was the only message on the other key, Sparrow I. The two encodings differed in certain respects - one had the figures in German while the other used the letter for figure substitution of the "J's" - but it was very difficult to account for the existence of a separate key. From our point of view this process had the advantage that, if the Nalm failed on Sparrow II, we could run it on Sparrow I and if it came out proceed to II by re-encodement.

The Nalm continued to appear almost until the end of the Italian campaign, but in the closing stages it did not come out. The last day broken was an odd one in February 1945; but isolated breaks of a key of this type were valuable as a check on the enemy I activity, and Sparrow had by this time played its small part in the maintenance of Allied security.

1·806 THE BALKAN ARMY KEYS

1·8060 General

The Balkan theatre throughout the war was full of the excitement which one expects from this turbulent corner of Europe; but the fact that it never became a major Anglo-American land front like North Africa and Italy meant that Balkan affairs took a secondary place to weightier and more urgent commitments. In 1941 and 1942 following the German occupation of Greece and Yugoslavia a considerable volume of Army traffic was intercepted from these regions, but it was not till February 1942 that some cillies gave decode evidence that this activity was in connection with operations against the partisans. A single day's traffic was to readers hardened to cynicism by constant press and radio reports of guerilla activity quite sensationally illuminating. In one day German units had been engaged in half a dozen areas of Yugoslavia: bridges had been blown, trains derailed. It was obvious that large Axis forces were being used, and that with battle, ambush and frostbite taking their toll, they were having a most uncomfortable time.

The early breaks provided a good sample of the type of traffic which the Balkans produced almost until the end of the war. Clearly it could not compete in importance with material dealing for instance with Rommel's African Army. So then when resources in bombes and cryptographers were small the Balkan keys were run only when fairly cheap and certain shots offered themselves.

1·8061 Before the Italian Surrender: February 1942 - September 1943

A penchant for nearness cillying by some of the Balkan stations was noticed in February 1942 and skilful exploitation - particularly difficult with this type of cilli - led to an average of four to five breaks a month on cillies, cillies plus beginners, and in one or two cases, on cribs, throughout March, April, May and June. The last of this series of cillies appeared at the beginning of July, and thereafter cillying ceased. In this period no first-class crib had been observed, and bombe-time did not permit of weaker shots. The Ravens, as the Balkan keys were generically named, were therefore lost to us from early in July. The precise distribution and function of the keys was not at the time clear, but it is fairly certain now that Raven I was the key of A.O.K.12, with Raven II as the associated Staff key; while Raven III, which was actually the first of the group to be broken, was perhaps some special key for an operation.

Raven I and II retained their importance as the keys of the senior unit in the area until the surrender of the Italians in September 1943, although A.O.K.12 during this period turned into Heeresgruppe E, and the key name presumably changed too. With the institution of a permanent Crib Room Research Section and the arrival of numerous bombes at the end of 1942, the stage was set for the breaking of Raven on cribs. And the appearance every day of a very long message from O.B.S.O. (Oberbefehlshaber Südost) suggested a possible means of entry. A number of examples of the O.B.S.O. Tagesmeldung had been seen on the days broken in the March - June period, and it then began with a long and highly variable address. However, on a November Mallard day, which owing to a compromise carried some of the Raven traffic, it was seen to begin GEHEIM X TAGESMELDUNG VOM (Date).

It was thought, therefore, not improbable that on some days it might begin flat with the Tagesmeldung, and a "directed boil" was carried out on the messages of December and the first week of January. The number of crashes was less than the random expectation, and one or two shots on different days soon resulted in a break. Two cribs were then revealed, both more reliable than the O.B.S.O. Tagesmeldung, the Supersloda Tagesmeldung, and even better, the Lagemeldung. Both these were daily reports from German Liaison Officers with Italian formations, and together with the O.B.S.O. Tagesmeldung enabled a grip to be kept on Raven for many months. None of these were reliable, and when they were all out of form many days passed without a break; but they always came back again to the known variations. The O.B.S.O. Tagesmeldung had the additional merit of occasionally being sent in Codfish, which offered the possibility of breaking by R.E. Such R.E.'s were always technically difficult on account of the punctuation differences between the ciphers; and in this case especially so because the Enigma version sometimes omitted portions which appeared in the Fish. However, analysis and practice led to increasing success, which became even more pronounced when the message began to appear on a new Balkan key, Buzzard.

Buzzard was broken on cillies almost on its first appearance on April 11, 1943, but traffic was very small in quantity until May, when a few more days were broken on cillies and revealed the daily O.B.S.O. Tagesmeldung R.E. into Raven. The reason for the introduction of the Buzzard key never became clear, and its German name was not discovered. Buzzard tended to be used in the northern Balkans - mostly in Italian occupation - while Raven remained popular in the south. But all major German formations throughout the area apparently possessed both keys - the commanders in Crete and Rhodes, for instance, possessed Buzzard although normally using Raven - and the only plausible theory advanced was that Buzzard was intended for liaison with the Italians, while Raven was issued only to German staffs. At any rate Buzzard mostly came from German liaison officers with Italian groups; while Raven surely could not have been in Italian hands when it contained such uncomplimentary remarks about them as "It is deplorable that again the Italians are trying - - - - - to make fools out of us and get what they want behind our backs"! (Raven II, 13/5). Whatever the reason for its use, Buzzard throughout May and June passed a large volume of traffic and was a most interesting problem, with occasional cillies, one or two cribs which could be attacked in different ways, and sometimes R.E.'s from Raven or Codfish. The cribs by this time both on Raven and Buzzard mostly began with wahlworts and therefore were less expensive when the ending could be used instead. Hence much ingenuity was employed in attempts to forecast the serial number at the end of the O.B.S.O. Tagesmeldung and its companion mid-day report, the Mittagsmeldung. If a version appeared on Fish, then the number would be known, and a plausible shot on both the Buzzard and the Raven would be the popular ending, as DREISEQSSIEBENFUENF GEHX or DREISEQSSIEBENFUENF STRIQ VIERDREI GEHX. If the number was unknown, one could at least forecast with some degree of probability the first two figures, and then make use of the standard end of the signature immediately preceding; one would then stagger ROEM EINS ANTON STRIQ OTTO EINS NUMX DREI SEQS and run it in the positions which required a reasonable number of letters following to account for the other two figures and the variations of GEHEIM.

With the disappearance of Buzzard the amount of traffic on Raven naturally increased and early in July new cribs from Rhodes began to score so that July and August both saw most days broken.

"Rhodes C" and "Rhodes A" were the IC and IA reports from the German staff on the island; normally there was nothing to say and the IC report was in the form (Address) MORGENMELDUNG (VON) (Date) KEINE BESONDEREN VORKOMMNISSE (Signature). Thus a plausible attempt could be made at writing out the whole message.

Raven I, then, was broken with increasing frequency as the year progressed. Meanwhile the more secret traffic was difficult to deal with because more than one key was involved. By analogy it should all have been sent in Raven II, but in practice many of the stations preferred Merlin (later known as Falcon II). Merlin was broken for the first time in May, when it was realised that it was a Staff key, by the process of running a number of messages from Susak on the beginner GEHEIMEKOMMANDOSACHE; the evidence of a crash analysis suggested that this was the best station and so it proved. Occasional Merlin days from May to September were broken in this way; whenever there was enough traffic to make an attempt worth while shots were made with normally about 20% of success. Raven II was treated at first as a rather different problem, for in June it gave us our first manifestation of a peculiar rule of the German Army Cipher Office which lasted until the end of the war, namely, that all Armee Staff keys should have the same discriminants. When traffic with "Albatross II" discriminants first appeared in the Balkans and failed to decode on the Albatross key, it was assumed that the two keys were basically the same with some minor difference such as a changed ringstellung, and great efforts were made to break into a message on such assumptions. Eventually "Albatross II (Balkans)" (i.e. Raven II) of September 5th was broken on the bombe on the beginner GEHEIMEKOMMANDOSACHE and the key was found to bear no resemblance to that of Albatross II of the same day, which fortunately was also out. It was soon realised that all Armee Staff keys were being allotted the same discriminants, and in future the fact enabled us to recognise Staff traffic more easily.

1·8062 Surrender of Italy: Appearance of Wryneck: September 1943 - November 1944

The imminent surrender of Italy at the end of August caused the Germans to reorganise their Balkan forces and Panzer A.O.K.2 was brought from Russia to direct the divisions in Yugoslavia, while Heeresgruppe E was left in charge of Greece in the islands; both groups being subordinate to the C.-in-C. with his staff, Heeresgruppe F, at Belgrade. In spite of these precautions, the situation caused by the announcement of the Italian surrender was chaotic; in most places the Germans took charge according to plan. But at Tirana the Italians took the German liaison staff prisoner, while on Rhodes there was severe fighting before the Germans finally took charge. These two events made the key position extremely complicated, for all the existing keys were believed compromised at Tirana, while the best Raven crib was no longer sent because there was now something to report from Rhodes. Raven therefore became very much smaller in quantity and throughout September it resisted all attacks. Meanwhile, Wryneck, the key of the new northern army, Panzer A.O.K.2, had been identified, and broken on a short morning routine message which had been correctly guessed on the 21st of September to say in 27 letters KEINE BESONDEREN EREIGNISSE YY.

Other days were broken on variations of this form - including more than once the solecistic KEINER BESONDERE EREIGNISSE - sometimes with the addition of some form of the signature ROMA EINS ANTON; and some days early in October were broken on cillies when one operator for a period used the setting PAU for every message.

Meanwhile Raven I 30/9 was broken on keyboard oillies, and revealed the form of the Rundspruch, a daily broadcast from Belgrade in both Raven and Wryneck giving details of Allied preparation for invasion of the Balkans.

From this point the Raven-Wryneck position became increasingly stronger. Both keys developed excellent cribs, Tagesmeldungen from the 114th Jaeger Div. and the 118th Inf. Div. being particularly good on Wryneck, while the old Rhodes IC Morgenmeldung and a similar "Nothing to report" message from Cephallonia could be expected to break most Raven days. The Rundspruch R.E. was easy when one of the keys was broken, and the Rundspruch itself was a passable crib in three-day cyclic form. To make things simpler still, the Raven and Wryneck keys indulged in some odd repeats, almost the only examples of this form of laziness which were ever found in Army keys. Raven in October and November repeated its stecker with some small alterations after fifteen days; Wryneck did the same in October, November and December and in addition in these months the wheelorder and ringstellung repeated themselves in blocks in such a way that by December it was possible to predict the wheelorder nearly every day and also the letters of the ringstellung. With a stecker repeat for the last half of the month, it was possible to write down the wheelorder and stecker and to find the ringstellung by trying the six possible permutations of the known three letters; and therefore, for a short spell Wryneck was passed from Research to the Watch so that the traffic could be handled currently.

Raven was broken nearly every day in November and then in December most annoyingly split into three keys. Of these one, E/6315A, passed the Rundspruch and nothing else, another, E/3730A, consisted of the Cephallonia crib and other traffic on the same frequency, while the third contained the bulk of the traffic, and clearly from this point was the key referred to as Maschinenschlüssel Aegaeis Süd. The loss of two of the best cribs left Raven breakable only on weak cribs and only a day or two in each week came out. There was a revival in March, when a third report from Rhodes broke several days, but this faded away, and from the beginning of May no traffic was read on the key for many months.

Meanwhile Wryneck I went from strength to strength throughout January, on three days the two best cribs, the Paulmeldung and the Monikameldung, which by this time both began TAGESMELDUNG coming in depth. This remarkable occurrence, which of course gave us 100% certain cribs on all three days, was due to the extraordinary coincidence that two different operators both became attached to the same message setting, LOS. On the 31st January the Monikameldung was sent in Wryneck II, which gave us our first break of the Staff key. Three routine messages turned out to be useless as cribs though interesting since they provided Y Intelligence derived from decodes of Tito's traffic. Cryptographically they were not entirely valueless, for during June and July they were occasionally re-enooded into Puffin II for the benefit of the armies in Italy; and when there was no information to give, a short message was sent in Wryneck saying something like SIE HOEREN UNS WIEDER UM..... UHR. The R.E.'s, however, were fiendishly difficult, while the little messages giving the QRX - times employed so many variant forms that they could rarely be used. The initial Wryneck II break was nevertheless not unprofitable, for it showed that at least some of the messages ended with the standard G-Tails (STRIQ VIERVIER GKDOS GEH(X)KDOS) which had been tried before but not apparently on a sufficiently large scale. Henceforward a certain amount of Wryneck II was broken by the the G-Tail method until the final disappearance of the key

late in 1944. Wryneck I with its heavy traffic was usually breakable too if enough messages were run on Geheim Tails. and from time to time when the cribs had bad patches this method had to be employed, notably in May and June. The June break restored the position, and from then on until December, four or five days were broken nearly every week on various cribs, mostly operational reports from the Corps under Panzer A.O.K.2.

1.8063 Arrival of Russians and New Balkan Set-up, November 1944

In November 1944 the Army with some of its Corps turned to face the advancing Russians and was subordinated to Heeresgruppe Süd, so that Wryneck became an Eastern Front key rather than a Balkan key. The result was that the traffic dropped to only a few messages per day, and only a few Wryneck days were broken in 1945.

Large parts of the forces which had been under Panzer A.O.K. 2 were now subordinated to Heeresgruppe E, which in consequence was once more allotted an Armee key and Staff key. These were given a new name, Quail, as the old name Raven was still in use for the Aegean key. December saw the gradual transference of some of the cribs from Wryneck to Quail, as units were re-subordinated. Annoyingly, one very good one went over to the little used general area key, Emu II, the Heeresstabsmaschinenschlüssel Süd. However, there was yet some semblance of order before the end. Wryneck and Emu II virtually disappeared, while Quail with often as many as 100 messages a day was broken with increasing regularity in January and February 1945 until finally the engulfing Allied armies overwhelmed the area and all the Quails and Wrynecks in it. The last Balkan break was an April Raven day, but it was like the many Ravens broken in December and January a bird of tattered plumage, a skeleton of its former self. In 1942 and 1943 we had read of ambush and reprisal from Hungary to Greece, from the Aegean to the Adriatic. In 1944 and 1945 Raven told of the two small beleaguered garrisons of Crete and Rhodes, well-provisioned and comfortable, disturbed only by the fear that unsympathetic islanders might resent the ease in which they were quietly waiting for the end of the war.

1.807 THE WESTERN AIR KEYS

1.8070 General

The story of the breaking of the Western Air keys is in general one of the most interesting examples of the ability of the cryptographers to exploit changing military circumstances with the minimum of delay. Allied war plans and Hut 6 successes moved side by side. The period between the fall of France and the beginning of the great air offensives of 1944 saw no breaking of Western keys except Red and Snowdrop (Masch. Schl. West. later Lgau West Frankreich). The whole emphasis of operational work was on the Mediterranean. Western keys were for the most part problems of Research, and it was realised that an Allied landing in the West would lead to a remarkable growth and shift of keys, and that the changes could not be completely predicted. It was only in the period from February 1944 to D Day, that our plans for exploiting the Western keys could become a little more clear, and it was felt that we should have to start afresh on D Day itself, hoping for large numbers of re-encodements, and being prepared to see the relative decline and fall of Snowdrop within a short period of the beginning of the offensive. Snowdrop and Red had been the objectives of our attack on the Western keys before D Day: it was realised that the former would go as the main cryptographic pivot, and that Jaguar, the key of Luftflotte 3 in Paris, would usurp its place. The assistance of Sixta was invaluable at this point. They had a much clearer idea of probabilities than we had.

D Day brought the expected change in emphasis in the Watch from Mediterranean to Western Air keys, and it had many surprises as well. The Flivo key, Ocelot, began to claim prior attention from the early days of the Normandy bridgehead, and soon jumped right ahead of Locust, the key of Fliegerkorps II, just as Puma had leapt forward in Italy. From the first landings to the drive across the Rhine, the number of German Air keys and the volume of German Air traffic never reached the same proportions as it did on the days immediately after D Day. Many keys were transformed or absorbed - Cricket and Ocelot, and Wasp and Cockroach being the chief. Towards the end of the war, there was a further shift in emphasis in the work of the cryptographers towards the Luftgau keys of Germany itself.

The work on the Western Air keys can be treated as a coherent whole, in much the same way as the work on the African Army keys. It was always the chief operational G.A.F. task of the period. To undertake it, large reserves of staff were built up in 1943. To carry it through, internal changes of organisation were frequently made. Towards the end, the strain of Reflector D and Enigma Uhr made this job particularly hard, but the fight continued until the end of hostilities solved many imminent difficulties, and released the cryptographers from a problem which was becoming very awkward to handle.

1.8071 The Breaking of Snowdrop

Snowdrop, the key of Luftgau West, was the only specifically Western Air key broken regularly before and after D Day, until the days of the German collapse. In 1942, despite many black patches, its battery of short reports provided useful material for Research, and in April 1943, it was considered to be in a sufficiently flourishing condition to be handed over to the Watch.

Its heyday was shortlived. In June, a wireless standstill order was imposed in France, and this killed most of the cribs, most of the practice messages, and all the operational traffic. Snowdrop went back to Research via the Qwatch, to be broken intermittently until it was ready to be returned to the Watch in March 1944. Its return was facilitated by the sending of a good crib alternately in Red and Snowdrop, and by a surprising increase in the number of routine Tagesabschlussmeldungen. Its value in the events around D Day was surprisingly high, but the prophecies that it would not outlive the successful onslaught of the Allied armies proved substantially correct. From being the key of Luftgau West Frankreich it eventually became the key of Luftgau V with headquarters at Stuttgart, and the key persisted, on a small scale and of minor importance, almost until the end. The last break was on April 15, 1945. The history of Snowdrop spans the change from the period of German supremacy in the West to its final eclipse. The routine Seenots, Zahlsprüche and Tagesabschlussmeldungen coming in clusters over long periods of time were the cribs of a nation resting on its laurels, the symbols of the serenity of an Air Force in comfortable occupation of a conquered land. One of the longest lived and best known cribs came from the Channel Islands. "Flak Jersey" never was a good crib, but its continuity in face of external changes was of considerable use. The turn of the tide in the West was marked by the German wireless silence, and then with the Allied landings, Snowdrop became vitally operational, passing as many as 820 messages on one day (June 9th). The Raffs, messages describing the state of aerodrome runways, were the swansong of the key, and in its Stuttgart days, little was left except re-encodements from other Luftgau keys.

1·8072 The Pivotal Importance of Red

Before D Day the main pivot of the cryptographic exploitation of the Western Air keys was, as in so many other cases, Red. As a general key, it provided frequent re-encodements into Snowdrop, and both W/T experts and cryptographers realised that the chances of getting into other Western keys were essentially dependent on re-encodements from it. The preparations for D Day in the Air Watch were mainly concerned with the refinement and development of kissing technique. The growth of a re-encodement complex was noted and exploited some months before D Day. On February 16, 1944, Jaguar, the key of Luftflotte 3, was broken on a re-encodement from Red. This was the beginning. February saw an entry into Tulip and Lily from Jaguar, and in March a slightly firmer hold was secured on Jaguar by the discovery that one of the small German LN. units in the Vosges was using Snowdrop and Jaguar on alternate days for the transmission of its small battery of cribs. The value of this Zoo group (so called because the code names used on it were Hippo, Maus and Muffel) was proved not for the first time. It had already enabled us to break many Red days early and cheaply, despite the queer habits it occasionally acquired, such as using its own key Aster, or using Aster and Red on alternate days. Now its peculiarities could be put to real use, and Snowdrop and Jaguar were both sent from Research to the Watch. In this way experience on Red was utilised to break other keys. Quite apart from this information and the value of re-encodements into Red, Red was a Western Air key in its own right. Two days after the first landing in Normandy, the Red traffic total went up to 809 messages.

1·8073 The Further Growth of the Re-encodement Complex

In the days before the invasion, much of the W/T picture was sketchy, and, in particular, the existence of some keys was regarded as problematical. This particularly applied to Cricket, the key of

Jagdkorps II. Its existence was in doubt, and traffic was closely tied up with Blue, the general practice key, which was thought to be part operational. This problem was cleared up by re-encodements, which enabled us to get the situation in hand on the eve of the offensive. Blue was broken on March 18th on a re-encodement from F/Blue, and Cricket was broken exactly a month later on a re-encodement from Jaguar. In April, a series of Tagesabschlussmeldungen on Lily, Snowdrop and Cricket were sent out in consolidated form in Jaguar. This unique form of re-encodement was of considerable value. On the 27th of April, Wasp, the key of Fliegerkorps IX, came out on a re-encodement from Legation Fag to Red. These various breaks justified the transfer of Cricket, Wasp, Lily and Lucust to the Watch in May 1944, though Locust was impossible, and Wasp unamenable, and the rest of the keys entirely dependent on re-encodements.

1.8074 D Day

The effect of D Day on the keys in France was much as had been expected. There was first a vast increase in the amount of traffic

	5th	6th.	7th	8th	9th	10th	11th
Red	324	459	501	546	809	611	462
Snowdrop	209	357	611	706	820	678	785
Jaguar	129	180	231	356	584	625	491
Crioket	31	168	219	239	328	271	249
Wasp	17	23	28	72	49	118	31
Locust	19	110	221	81	167	218	215
Ocelot	-	-	-	152	179	122	123
TOTALS	729	1297	1811	2152	2936	2643	2356

Expressing it more colourfully, the Red total on the 9th or the Snowdrop total on the 9th were each higher than the total traffic of all these groups on the day before the invasion.

There were other changes too. The Tabs messages, which had been the backbone of the previous attack, disappeared over night. Snowdrop was far more important and urgent than had been thought likely. Locust, the key of Fliegerkorps II, proved to be not one key but two, a large proportion of the identified traffic passing on Ocelot, the Flivo key of Luftflotte 3.

For some time, the only profitable line of attack on the keys lay in re-encodement. The task of investigating over three thousand daily kiss pairings became the chief task of the Watch, and when a key was broken, quite frantic efforts had to be made to secure complete entering, and to prepare the way for the discovery of new cribs. The crib position remained obscure throughout these early days, but there were sufficiently numerous re-encodements to give us samples of all the important keys (including Gnat and Wasp), and there were reasonable grounds for the hope that many of them would prove tractable after more evidence had been obtained.

1.8075 The Period of Regular Breaking

By the end of June 1944, the Western Air keys as a whole were in a very healthy state, and all major Air keys were being broken on cribs. The change was most marked on Lily, which was entirely dependent on re-encodements for the fortnight after D Day, but during the last ten days of the month, all days broken fell to cribs. Ocelot, Jaguar and Cricket all produced short messages of crib value, while Wasp developed a veritable battery of cribs. The shadow of D was not yet hanging over the West, and the successes in the routine Watch enabled the Watch

party to deal with more difficult keys like Firefly, the key of the German Paratroop Army, and with minor and somewhat curious keys like Armadillo (a home-made Sonderschlussel with consecutive stecker and non-Nigelian wheelorders) and Platypus (the key of Flak Korps 3 dealing with air security). The successes on the major keys in the period between the 6th of June and the end of the month are worthy of quotation:

Snowdrop: all days broken; (25 breaks);
Wasp : all days broken except the 7th and the 11th;
Lily : all days broken except the 17th and the 27th;
Jaguar : all days broken except the 14th;
Cricket : all days broken except the 7th;
Ocelot : all days broken except the 9th.

The total score was 143 breaks out of a possible 150. In the last six days of the month on the keys mentioned above, twenty four breaks were made before 0100 G.M.T. on the following day. The average times of breaking were in some cases extremely early:

Ocelot: 1055
Snowdrop: 1030

being outstanding.

In a sense this was the peak month of our successes on the Western Air keys, for, although many major successes were to lie ahead, the elements which were to upset the hold on the West were already beginning to be noticable in July. On July 10th, the first messages to be sent on Enigma Uhr came on Jaguar and Cricket without warning, and they certainly slowed down the breaking of Jaguar, which had never been the best of keys to deal with. On August 1st, [illegible] regarded as crisis day, the first use of Reflector D on the Western keys affected Jaguar again in particular, and many other keys as well. On the 5th of August, Wasp appeared to go over entirely to D, and even though B messages on the Nosegay Fag enabled us to recover the days at the end of the month without much difficulty, none the less the circumstances inspired little confidence in the future. On August 1st, Ocelot changed its Funkplan, and though this W/T change had little effect on breaking, it was an unpleasant foretaste of things to come. And these changes, technical and otherwise, came at a time when a rapid and all-sweeping Allied advance was having a very bad effect on the stability of both cribs and keys. Many cribs went about this time, the most lamented of all being the Zoo cribs on Snowdrop. Snowdrop itself as a key was compromised in the second week of August, and two or three keys were put into use. Although Snowdrop traffic was to reach high levels again with the landings in the south of France, the position of Luftgau West Frankreich had been settled for good and all with the breakthrough at Avranches.

These elements of doubt and uncertainty were mainly incipient however. Some of the most valuable work of Hut 6 was done in this period of Allied drive and advance. Ocelot was broken regularly, mainly currently, for every day in July, and all days but one in August. Its message totals were high, and its intelligence value high also. Time tests were taken at this period to make sure that the messages went through to Hut 3 with the minimum of delay. The average times of breaking are worth quoting:

Week ending July 8th: 1430;
Week ending July 15th: 1245;
Week ending July 22nd: 1905;

Week ending July 29th: 1330;
Week ending August 5th: 1310;
Week ending August 12th: 1500;
Week ending August 19th: 1640;
Week ending August 26th: 1650

Here again this was the peak period of success.

Despite a considerable amount of Jaguar traffic on D and Enigma Uhr, every Jaguar day in July and August was broken, 33 of them currently. Only eleven Wasp days, despite the period of universal D, remained unbroken. Taking into account the Snowdrop compromise, the position on that key was as good as it could have been. 42 Firefly days were broken. None of them were easy, cribs were few, and cillies marked the best line of attack. A firm grip was maintained on Gnat until it disappeared with the Allied advance from Angers to Rheims. 26 breaks were made on Lily, many of them of considerable value because of the connection of Lily with V-weapon supply. In fact this was the period when Hut 6 was able to supply all the important operational intelligence to the Allied commanders. After September, the German Air Force itself was effectively finished as a major factor in holding back the Allies or securing the safety of the Reich.

1.8076 Changes in Emphasis

With the Allied advances to the German frontier, the work of the Watch began to be based more and more on the German keys.X The W/T position of the Western keys was itself radically changing. Luftflotte 3 (Jaguar) moved from Paris to Rheims, from Rheims to the Coblenz area, from the Coblenz area to near Limburg. Its title changed to Luftwaffen Kdo. West. Luftgau West Frankreich (Snowdrop) and Luftgau Belgien-Nord Frankreich (Lily) were absorbed into the Reich structure by the division of Luftgau VII. They became Luftgau V and Luftgau XIV respectively. The remaining Dutch airfields were subordinated to Luftgau VI. Luftflotte Reich (Hyena) grew rapidly in importance. It was a re-encodement between Jaguar and Hyena that cleared the air after Jaguar had become particularly difficult during the early weeks of September. At the end of the month, Daffodil seemed to be taking a more important place at the cryptographic centre with re-encodements to Lily and Snowdrop as well as to Hyena, Cockroach and Gorilla. With the withdrawal to Germany, the numerous Festungen, left behind by the Germans as strong points in the rear, began to use hand-made Notschlussel. Snowdrop cast off a number of such offshoots. Not-Guernsey, for instance, made its first appearance at the beginning of October. The system was to spread to all sectors, both Air and Army, but it began in the West. On December 1st, Daffodil split into its constituent Luftgau keys, a natural and somewhat surprisingly delayed change, which finally placed Lily, Snowdrop and Aster (Luftgau VII) in the German orbit. This left only two of the original Western keys, for one of the welcome changes of the beginning of November had been the amalgamation of Cricket and Ocelot. Jaguar and Ocelot were now left as the two basic keys. Wasp, mainly on D, was broken from time to time (e.g. October 28th), but until Jagdkorps I was disbanded and some of its networks taken over by Fliegerkorps IX on March 1,1945, there was no long period of breaking.

1.8077 The Decline of the West

Until the end of 1944 and the beginning of the new Allied

X See separate section on the German keys.

offensive into Germany, the Western operational keys, now properly including Cockroach (Jagdkorps I), were in good operational trim, despite technical difficulties like Reflector D and Enigma Uhr, and despite a growing number of key compromises, which at times made the W/T position very complicated. At other times, they helped us much more than they helped the enemy. For instance, Jaguar of January 1945 repeated the Jaguar B key of December, and though this was not solidly broken then, there was little difficulty in filling in the gaps left. Similarly, one subscriber on Ocelot in January 1945 had not got the new month's key, and obligingly used the previous month's key backwards, giving daily letter-to-letter re-encodements into the current key. Such mistakes on the part of the enemy were frequent in 1945, and together with the capture of key-sheets enabled us to keep a precarious hold on keys, which might otherwise have slipped from our grasp. By such improvised methods we were compelled to live through the few months before the great link up of Russians and Americans and the final victory of the Allies. None the less, in 1945, 108 breaks of Jaguar were made, and 105 breaks of Ocelot, out of a possible total of about 120 days. Only one Cockroach day was missing until it became known as Wasp at the beginning of March, and thereafter 39 Wasps were broken. Breaks of Ocelot were becoming increasinly expensive. An examination of bombe hour figures on the key at different periods throws up some interesting results:

	Breaks	Bombe Hours	Hrs.per Break
July 2nd - July 29th . . .	28	1150	41
July 29th - Sept.2nd . . .	33	2410	73
Jan.28th - Feb.24th . . .	28	6609	236
Feb.25th - March 31st. . .	33	8892	269

All these figures count only one key break per day, e.g. when there was a Jaguar I, a Jaguar C and a Jaguar IIA, Jaguar IIA is counted, because it was the main Jaguar key. The same applies to the counting of Ocelot II and Wasp II. These breaks were accomplished against a fluid war picture, in which the decline in the importance of the Luftwaffe had greatly reduced the intelligence value of the operational keys. Traffic totals reflected the changing fortunes of war, and towards the end dropped phenomenally - Jaguar, for instance, from a daily average of 233 messages at the end of March to 81 messages at the end of April, and 24 messages for the week ending May 5th.

The main cryptographic theme of this period was the hard fight against D. When the Allied troops landed in Normandy in June 1944, D 15 was in use; by May 1945, we had reached D 333. Early in March 1945, it seemed that because of the use of D, and the scarcity of satisfactory B cribs, Ocelot was certain to go. A stray re-encodement from Jaguar into a key that was hoped to be Ocelot providentially came out. It revealed new cribs and a considerable amount of B traffic. The Jaguar which gave the re-encodement was itself a captured key. By the end of March, Jaguar, Wasp and Ocelot were almost wholly on D, and the future seemed very black indeed. April saw a prevarious but happy start. Ocelot was broken on B traffic, the D recovered, and a re-encodement into Jaguar came out on Duenna. Each new D period in April came as a critical turning point. The three keys were now hanging together as they had never done before. Operational messages like Erdlages and Aufklärungen were re-encoded freely between all three keys, but they had a habit of not being there when they were most required.

The May prospects for breaking seemed depressing, but the difficulties we had to face were paralleled by those of the Germans. Faced with the problem of distributing fresh cipher material, the Germans were having to rely increasingly on rehashes of old keys.

In May, part of the Ocelot network was to use the April keys over again in a hatted order. May Jaguar was used in April by units of Flieger Division 14, and re-encoded into Ocelot and Wasp. Wasp itself was mainly on D, its two bad cribs were both D, and it was dependent on occasional re-encodements from Raster. Despite all the difficulties, the way in through new lines of attack in May was clear, and there is little doubt that if we had once made an initial entry, a break into the other two keys would have been possible.

1·808 THE WESTERN ARMY KEYS

1·8080 General

The German Army was well trained in the first golden rule of cipher security, that no traffic should be sent over the air unless it is absolutely necessary. Consequently the history of Army keys everywhere is a story of spasmodic bursts of traffic with long periods of silence, and often no continuity between the traffic of one period of activity and another.

The Western campaigns thus provided three glorious periods - the initial landings, the drive through France, and the final battles on both sides of the Rhine - in which most of the Heeresgruppen and Armies engaged were on the move and had to use wireless communication. In such times the Army Watch spared no effort to make hay while the sun shone, and the supreme importance of the intelligence given meant that bombe time was always available if required. The stress and movement of these times was the exact reverse of the conditions in which one usually found cribs, for normally these came from units which were settled for long periods in one place, and had fallen into a groove. Consequently the breaking of Western Army keys was a hand-to-mouth affair, dependent upon the closest inspection of current decodes, and allowing plenty of scope for ingenuity.

The number of keys issued to units in the West was normally out of all proportion to the amount of traffic actually sent over the air. In addition to the general operational keys, the Bantams and Puffins, and the general supply key, Peewit, every Army had its own key and staff key. As there were always at least five Armies in the West, and in the later stages seven or eight, it might be thought that the Armee keys alone would present a formidable problem from sheer weight of numbers. In fact there was very rarely any great volume of traffic on any one Armee key, and apart from the very early days of the invasion, when there was plenty of Duck from A.O.K.7, and after Avranches, when Panzer A.O.K.5 began to send Dodo, we scarcely saw any Armee traffic. When the current keys of A.O.K.19 and A.O.K.1 (Gosling and Swan) were captured in August, it was unusual to see more than a single message decoded, and sometimes there was not even that, and this was when the two Armies were heavily engaged and on the move. Panzer A.O.K.6 (Whimbrel) was more forthcoming after Von Rundstedt had launched his counter-offensive in December, and with thirty or so messages a day of high urgency it was well worth having. In this case the first two breaks were the last, for no sooner had they been achieved than the offensive ended and the Army was withdrawn and sent East; a typical example of triumph and disappointment for the Army cryptographers.

1·8081 Before D Day

Unlike the Air keys, the Western Army keys passed virtually no traffic of significance before D Day. The keys were in existence - we had references to them in other traffic from time to time - and were occasionally used in large-scale W/T practices which were sometimes coincident with Army manoeuvres. During these practices, which usually lasted for a week or rather less, numerous frequencies appeared passing quantities of traffic in several different keys, the messages mostly being

very short and having every appearance of Quatsch. In the days of discriminants it was fairly easy to identify the Armee keys by area and it was recognised that there was more than one general key in use. After the dropping of discriminants identification of the keys was very difficult, a state of affairs which persisted throughout the subsequent history of the Western Army keys.

The first break in the West was in January 1944 when a routine message from Brussels had a cilli to MIX with TOM outside, and the day was broken on MIX plus a stagger of the date. Disappointingly little traffic decoded, and all of it was clearly practice. The routine message proved to be simply the German High Command Communique, encoded and transmitted presumably for practice, and one other day was broken as a result of this discovery. An interesting point about the first 320 Group break was the fact that the key had the same stecker as one of the broken Quince days of the same month, suggesting that the key was an S.S. key, for S.S. keys sometimes bore a relationship to each other, but were never known to be connected with Army keys.

A big W/T practice in February led to the first genuine break of an Army key. "Chicken" 27/2 was broken on some cillies plus a stagger of VIERVIER, and proved to contain a quantity of operational practice, i.e. traffic which looked in every way like the real thing except that somewhere in the text appeared the words X UEBUNGSSPRUCH X or X UEB X. In addition there was a little genuine traffic and the whole dealt with supply matters. It is quite clear now that "Chicken"27/2 was the first break of the key which was later known as Peewit, the supply key in the West.

Although this exercise lasted for over a week, and the Chicken decodes seemed to hold good crib prospects, no other days were broken at this time. No further successes were scored until the beginning of May, when the procedure of running the standard Geheim and Gkdos Tails on multi-teile messages brought breaks of Bantam I 3/5 and Bantam II 5/5. The traffic was at the highest level, signatories including O.B.W., Heeresgruppe B, A.O.K.7 and A.O.K.15, and it included genuine as well as operational practice material. This was our first intimation of the fondness of O.B.W. for the standard G-Tails, but we received confirmation of it in yet another big exercise at the turn of the month, when a Bantam II and a Bantam I came out on these endings. Another Bantam I day, 30/5, came out on cillies.

These then were the only glimpses we had had of Western Army traffic prior to the invasion, although there was one special purpose key which was being broken fairly regularly, namely, Nightjar, the key of the military occupation authorities, who had a big wireless network throughout France. Prior to the invasion the traffic passed was mostly practice, but even then it was clear that the object of it was speedy reporting of sabotage to communications, especially landlines, so that alternative routes could be quickly devised and repairs set under way.

Nightjar was first broken in April when a March day came out on a Geheim Tail run on a long routine message which proved to be a LAGEORIENTIERUNG. Incidentally, the first break was exremely lucky, for the message scarcely ever ended in this way again: however it was quite a good crib at the beginning, and broke many days until it finally disappeared two days after D Day.

i·8082 D Day and the First Breaks

Thus when D Day finally came, bringing with it floods of traffic, we had a very good idea of what keys to expect, but very little notion of what they would be saying. It was fairly clear at once that two or three keys were in use and that there was a good deal of re-encoding going on and it was very disappointing therefore when the first key broken proved to be a Y key having but little connection with the others. This was Pullet 8/6, which was the only key ever to be broken by a "Banbury Stagger", a method used where the same text was encoded at different positions of the machine at known relative distances.

However, success was not long delayed. Heeresgruppe B tried to send Bantam on the Jaguar star, which quickly resulted in a re-encodement from Jaguar as Luftflotte 3 possessed no Army key. A break of Duck I, the key of A.O.K.7, on a re-encodement from the Bantam, followed a few hours later, and Duck II, the Staff key, succumbed in its turn. All these were keys of 9/6 broken very quickly after the Jaguar had come out during the afternoon of the 10th. One promising lead into other days appeared, a IC Abendmeldung from A.O.K.7 which scored on the 11th and then not again till the 17th. From the 17th breaking of most days of Bantam I and Duck I, and some days Duck II proceeded until the fall of Cherbourg on the 25th. There were R.E.'s between Bantam and the Ducks every day, and it was a case of scoring one break on a day and then exploiting the R.E.'s. Bantam had a crib from the 1st S.S. Panzer Corps, while Kampfgruppe Schlieben in Cherbourg, which had lost all its keys except Duck II and Dolphin, the Naval key, obliged by providing R.E.'s from Dolphin and also by being sent several days Pullet keys in Duck II messages.

1·8083 The First Lull

With the fall of Cherbourg on June 25th, traffic which had fallen off considerably since the first few days of the invasion dropped to not much more than a trickle. However there were still one or two keys to be broken, for Nightjar was providing plenty of traffic and produced some cribs which enabledus to break almost every day in July.

Meantime a break of Peewit, the Western supply key, had been achieved on a depth-reading, and several long supply reports, coupled with a considerable amount of cillying, enabled us to break nearly every day in July. This was a most valuable key, for apart from the obvious uses of supply intelligence in a period of static warfare, there was a tendency for the enemy to fall back on his supply key when the operational keys were compromised; and thus at various times Peewit breaks decoded much that was normally on operational keys like the Bantams.

Two minor oddities were Penguin and Diver which provided innocent amusement for the cryptographers without, one feels, greatly increasing Hut 3's knowledge of the German Army. Diver was the special key used by the 319th Division in the Channel Islands, and was sometimes broken on its short nil returns. Penguin was one of the few Divisional keys which was ever identified. It was quite clearly an ad hoc cipher for use [illegible] of the 12th S.S. [illegible] there were only six

different keys - and two of those were very similar - which were used again and again. By the end of the third or fourth period of six days all but one of the keys had been broken on R.E.'s from Non-Indicator traffic or on cillies, and eventually enough cillies were collected from different dates to break the last day. Penguin lasted from the middle of June to the end of August, and for most of that time nearly all the messages were being read currently.

1·8084 The Breakthrough

On July 26th the American offensive in the direction of Avranches and the resumption of open warfare caused traffic totals to rocket to unprecedented levels. Some of the signatures of the Corps of which we had collected evidence in June gave some quick breaks, and R.E.'s from Bantam to Duck and day-to-day R.E.'s helped by carrying most of the traffic on the last two days of the month when most of the other keys had been compromised.

From now on two features stand out in the general confusion which followed the German defeat in France. First it became quite impossible to sort out the various keys in use, and therefore the Barnyard cover-name was introduced, the first key to be broken on a day being called Barnyard I, the second Barnyard II and so on. Generally speaking, all the traffic was tried on each key broken. which, while a heavy burden on the Decoding Room, was the only way of ensuring a minimum of delay in sending urgent material to Hut 3. Secondly, from the breaking point of view it now became possible to exploit C.B.W. (C.-in-C.West)'s tendency to use the standard secret endings to his messages, for C.B.W. was now consistently on the air passing traffic to the Heeresgruppen and Armeen. Meanwhile the landing in Southern France had brought Armeegruppe, or as it was later called, Heeresgruppe G on the air, and it soon became apparent that this station had a strong tendency to end his messages with the current days date. From this point until the end of the war C.B.W. and Heeresgruppe G were fairly reliable stand-bys whenever they appeared on the air.

With the spread of the war more general keys came into use. Bantam, Wehrmachtsmaschinenschlüssel West, remained in use between the main Western stations, but there was a tendency to use Puffin as an alternative. This was probably because O.K.H. was frequently on the air at this time, and although possessing Bantam, showed a strong preference for Puffin, which was indeed his own key (C. K.H. Maschinenschlüssel B). Falcon, too, began to be concerned with the western fighting, for as the exact counterpart of Bantam for the Home War Area. it was possessed by units like Heeresgruppe G who had now retreated right into Germany. With frequent compromises and a rapidly changing battlefront, it was usually impossible to tell which of these keys one was trying to break. Puffin was sometimes obvious when there was some Mediterranean traffic on the key, but this theatre was liable to the same fluctuations in traffic as the western, and days would pass without a single message being taken.

1·8085 The Second Lull: October

With the completion of the occupation of France and the reversion to static warfare traffic dropped once more, but the successes of August and September left us with two or three breakable keys which continued to pass a fair volume of traffic

E/Lorient was steadily broken until near the end of October, when the Fortress was transferred to the Naval Command, and the operational military traffic disappeared. Occasional breaks were secured afterwards on a long report on losses which was sent once or twice a month, but the interest of such a local key was never great. It was one of those keys which were broken because they were cheap and easy to break rather than because their intelligence value gave them a high priority.

Bantam I soon dropped to a trickle but was breakable most days owing to a routine re-encodement from Ocelot, sent on an Air frequency. This died at the end of October, but it lasted just long enough to give us one or two R.E.'s into Blunderbuss, the Western Railway key, upon which we were then able to obtain some sort of hold.

Blunderbuss (formerly known as RocketII) traffic was first read in August, when four days' keys were given us by a deserting cipher clerk. The decodes were unpromising and no progress was made; but the R.E.'s from Bantam at the end of October revealed one or two cribs which before they disappeared sufficed to break a few days and show the power of the ends of messages from Essen. From now on until the end of the war all messages from Essen were run on the ending SPRUQ ESSEN NUM (serial number), and many days in most months were accounted for. Obviously steady breaking was essential here, for otherwise one soon lost track of the serial number.

Culverin (first called Stephenson) was another Railway key which made its appearance at this time. A group was intercepted in Holland for a few days passing Non-Indicator traffic, of which one day was broken. Enigma was passed from the beginning of October, and a break was obtained on the evidences of the N.I. decodes.

The key was soon shown to be very easy to break, since only wheels I, II and III were used, and nearly all the messages said either

DURQLAUFXBEITHEIXRIQTUNGXHOLLAND

or

DURQLAUFXBEITHEIXRIQTUNGXREIQ

according to the direction in which the train in question happened to be going.

All these keys, however, were of minor importance compared with Falcon II, which was the great legacy of the breakthrough period. In some of the Barnyard breaks of that time multi-teile messages decoded which were routed from Berlin to the western Wehrkreis centres on the main Greenshank network. These messages discriminated to distinguish them from the normal Greenshank traffic, and it was fairly obvious that Falcon II was being used as the Staff key to Greenshank as there was no Greenshank II. This was extremely fortunate from our point of view, as Greenshank itself was almost unbreakable owing to the daily-changing Reflector D, but Falcon II possessed cribs and was on Reflector B.

A proportion of the messages in this key emanating from Berlin began with some variant of

GEHEIMEKOMMANDOSACHE AN STELLV GEN KDO RCEM.....
or AN WEHRKR(EIS) KDO RCEM....

The large number of variations of this beginner, coupled with the fact that much of the traffic had quite different and completely unpredictable beginnings made the breaking of Falcon II extremely expensive in bombe time, but the very high level of intelligence produced made it worth breaking at almost any cost.

Falcon II remained in this state of breakability until traffic finally disappeared at the end of March. There were periods of days and sometimes weeks when there was little or no traffic. But as soon as Berlin obliged by sending a few messages, the "Secret Head" method of breaking usually sufficed.

Parallel to Falcon II but with a different function was Falcon I, a key of wide distribution but chiefly used for communications within Wehrkreis VI. Long before D Day this key was being broken regularly on addresses, but interception was seriously affected by the introduction of encoded callsigns; and cover on the groups was dropped after D Day in favour of M/F traffic more closely connected with the battle. In August and September it was realised that some of the keys which were being broken as Barnyard were in fact Falcon I - odd messages taken on search from the Wehrkreis VI stations decoded - and a drive was instituted to improve interception. With encoded callsigns it was difficult to identify the stations on the group, and breaking, which formerly had been exclusively on addresses, would depend upon correct identification. By taking the best of the old addresses and running them on messages having a large number of different routeings, some breaks were obtained and it became possible from a combination of D/F, log reading, callsign continuities from breaks and observation of station idiosyncrasies to identify some of the main stations and thus make breaking not prohibitively expensive.

Falcon I was broken on most days from November onwards until the end of March. For the last two months or so we were permitted the luxury of two genuine cribs - an evening report on the position of the Allied armies, sent out by Münster to all stations, which had a useful address as well as a good signature; and a series of CQ messages from Münster, giving information on a variety of subjects, but most commonly on action in the event of landings from the air or on signals matters. The messages were recognised by procedure and either at the beginning or end announced themselves as SAMMELSPRUQ NUM (number). With good interception it was fairly easy to calculate the number, which went up one for every message.

At the end of March Münster was evacuated and the administration of Wehrkreis VI finally broke down. The key gave steady if perhaps unexciting intelligence concerning administrative supply matters in the vital Ruhr area over a long period and was of great cryptographic value in that it gave R.E.'s into Greenshank on the one hand and Bantam on the other.

Bantam as the main operational Western key still appeared spasmodically in bulk, but normally consisted of a steady stream of from twenty to thirty messages a day mostly on a star controlled by O.B.W., with the main active outstation at Münster. Hence the Falcon-Bantam R.E.'s which arose when one of the subordinate stations in Wehrkreis VI wished to send a message to O.B.W. and did via Münster. Both Bantam I and II were broken from time to time on the endings of messages from O.B.W., while there was a period in January and February when Bantam even had a crib, a short nil return of many variant forms which came from

a forward supply dump of Heeresgruppe B. The sender quite clearly tried to produce a different form of the message every day, and it was amusing to attempt to guess each one as it was used.

One other key was broken in this period. A break into Pigeon, the Western Y key for communication between German intercept stations and breaking centres, enabled us to maintain a grip on this traffic for two or three months, providing valuable information on our own ciphers. The tightening up in our own security which followed resulted in the disappearance of the Pigeon crib messages, which gave lists of Allied frequencies or announced breaks of our low-grade ciphers.

1.8086 The Final Battles: Heavy Traffic Once Again.

The long lull in Army W/T activity, which had lasted, apart from occasional short bursts of traffic, since September, was finally broken with the offensives to clear the left bank of the Rhine; and with the Rhine crossings and the subsequent open warfare the totals rose to their highest levels once again. As before C.B.W. and Heeresgruppe G were normally expected to provide us with at least one break, and other keys were broken by re-encodements. In this period, as before, keys did not remain in force long owing to frequent capture - or suspected capture - by our forces. The resulting chaos meant more keys to break than would otherwise have been necessary, for usually some of the stations went on using the compromised keys, while others obtained new ones, and others used some available substitute.

It is somewhat ironical to recall that in most of these supposed compromises the keys must have been first destroyed by the Germans. At any rate they did not normally reach us. But on one famous occasion when the Canadians captured the current Bantam I and Dodo I and II keys in August and sent them back in time for us to decode half the month's traffic currently, the Germans specifically stated that these keys were quite safe!

Puffin finally came into its own in the last days. This, the general O.K.H. key for use in the West (including the Mediterranean and Balkans) was used to a considerable extent in August and September when Puffin I, II and even III (the key used for Chefsachen messages of the very highest grade of secrecy) were included among the many Barnyard breaks. In the period of quiescence there were several occasions when Puffin had enough traffic from the various fronts to make it worth breaking; nd considerable bombe time was then expended on numerous versions of the cribs from Crete, the Morgenmeldung, Abendmeldung and Tagesmeldung which were sometimes sent from Crete to O.K.H. in the special Cretan key, Flycatcher, and thence to Heeresgruppe E in Puffin. A dozen versions on any one of these messages might offer no better than a 25% chance of success, which was not encouraging to the cryptographer, but nevertheless yielded success to the persevering.

There were long periods, too, when most of the Puffin traffic consisted of those broadcast Y reports which were such a feature of the German Intelligence system in the West. This type of traffic would occasionally succumb to a heavy exhaustive attack, for all the messages contained a serial number, usually in the middle but sometimes at the beginning or the end.

But at least one break very close to the day under attack was necessary, for otherwise the number would have lain within too big a range.

But the Crete reports and the Y messages were the cribs used in the quiet periods. Perhaps some of the most valuable Army intelligence came from the efforts of these times - from Falcon II, for instance, which outlined the building up of the new 6th S.S. Panzer Army for the December offensive and was a continual source of information on German defensive policy. But the exciting moments for the Army Watch were in the periods of traffic, with their crescendoes just after D Day, again in August, and finally in March and April. In these times the unit on which we worked was the message, or, if it discriminated, on its discriminant. We ran on the bombes anything which any of the messages might plausibly say; and when one came out, the others were tested on it. Some did not decode because they were on other keys and they were left to run until another key was broken. Thus in August and September on some days as many as nine or ten keys were broken; nameless keys, for they were simply called Barnyards I, II, III,....IX. Most of them came out on E.E.'s from key to key, which meant that those last in the chain tended to be broken two or three days late; but it also meant continuously exciting and interesting work for all concerned, with its aim to get a glimpse into the mind of a German commander, or cipher clerk, or both, and to do it in time to assist our own command.

1·809 THE GERMAN AIR KEYS

1·8090 General

It is difficult to write the history of the German Air keys except in the reflected light of the Allied advances of 1944 and 1945. Yet in 1942 and 1943, such advances were very remote. When the Germans were battling towards the Nile Estuary, and fighting along the banks of the Volga, Greater Germany was still secure, miles away. At that time, the German Air keys were distinctly a research proposition, occasionally providing some intelligence about night fighter defences or aircraft dispositions. Such was the case in January 1942, when Cockroach was wanted for radar information. The demand for this key soon went down, and it became a routine research commitment. Daffodil was as a rule even less valuable, and traffic totals were low over long periods. Both Daffodil and Cockroach (along with Hyena, the key of Luftflotte Reich, which first appeared in 1944) were not transferred to the watch until the eve of the Second Front, and Daffodil did not soar to really high intelligence value until the end of September. From that time onwards until the end of the war, the cryptographic exploitation of the German keys was made more difficult by disintegration, compromise, and increasing technical complexities.

1·8091 Research

The long period of research breaking of Daffodil and Cockroach in 1942 and 1943 can be told very briefly. Cockroach appeared at the beginning of 1942, after the splitting up of Red. At first it was the key of Fliegerkorps XII, which it remained until October of the same year when Fliegerkorps XII was renamed Jagdkorps I, the first Jagdkorps that appeared. In Research, it fell into the category of Cilli Keys, and the number of cillies and occasional examples of depth gave it a fairly interesting life. From the crib point of view, it was chiefly distinguished for its "Spruch" messages, although by 1943 it had acquired some of the standard cribs- particularly Gefechtsberichte - which were to serve until late in the war. On the whole, breaking was steady and unspectacular and we were helped considerably by key repeats. Daffodil appeared rather later than Cockroach. On May 1, 1942, Snowdrop (Lgau.Masch. Sohl.West) was restricted to France, Belgium and Holland, and a new key was introduced for North Germany and Scandinavia. For a month it was known as Snowdrop II, then it was given the name of Daffodil. Two months later a separate key was introduced for Norway, named Narcissus. Some Norwegian traffic continued to be sent on Daffodil in November 1942, but in general its use was now restricted to Germany and Denmark. On March 1, 1943, each Luftgau was allotted a separate key, and Daffodil became the key of Luftgau XI,* but two months later, all the German Luftgau groups, with one or two exceptions, went back to Daffodil again, which remained the general key until December 1, 1944, when it split up into seven components.

Over this long period, Daffodil traffic totals fluctuated considerably. In 1942 and 1943 totals were usually low, but a heavy air attack would lead to a great increase in the volume of traffic. Early in October 1943, for instance, there were

* There had been a Luftgau XI key issued in 1941 (Daisy), but it was never broken by Hut 6. For further details see Distribution and Use of G.A.F. keys.

heavy air attacks on Hanover and the Hamburg region. Traffic totals rose enormously, the intelligence value of the key rising also, and the cryptographic interest of Daffodil was enlivened by a bout of oillying on the part of the German operators. This was somewhat exceptional. For the most part the breaking of the key was not a thrilling or particularly rewarding cryptographic experience. Re-encodements were few, although now and again re-encodements from Red were useful, particularly when cribs were difficult. The first Daffodil crib - the Zahlspruch - was a day report on the number of practice messages sent and received. Luftlage, first used as a crib in the early days of 1943, was the foundation-stone of almost all regular breaking, and remained so until the end of the war. Its cyclical habits were a later development. Early in 1943, new cribs appeared on Daffodil, of which the best known were the Luftparks, and a spate of stecker and other key repeats gave some scope for breaking on these new messages. When Daffodil was transferred to the Watch in May 1944, it had already had a long history, and round about that time was being used throughout the area of Greater Germany.

One other point of interest was the periodical interchanges between Daffodil and Blue, the G.A.F. practice key (Luftwaffenübungsmaschinenschlüssel). Occasionally Daffodil cribs, like the Luftlage, would pass in Blue, and Blue Quatsch messages would pass in Daffodil. It was useful to break occasional Blue days to clarify the W/T picture.

Hyena, the key of Luftflotte Reich, was first broken in March 1944. At first it was thought to be merely an offshoot of Cockroach, passing on the Jagd.Div. 7 links, but later it was discovered that the key also decoded messages on Luftflotte Reich stars. Eight breaks of Hyena in the first week was perhaps the summit of Hyena's success. It was never so easy again to break as it was in March 1944, when the Cockroach Luftlage and the Zudet 3 both passed on the key as well as its own cribs, the weekly Tuning Programme and the daily Reichspruch. By the end of May, when Hyena was transferred to the Watch, it was in a much more tricky and unyielding condition.

1·8092 The Watch

The treatment of German Air Keys in the Watch and the Qwatch falls into three phases:

(i) from late May 1944 to August 1st;
This was the period when the keys were absorbed into the operational system of Watch and Qwatch breaking, when they were given Watch parents and Watch folders, and when they were examined currently by the routine shifts.

(ii) from August 1st to December 1st:
August 1st marked the first use of Reflector D on the German keys, and this radically affected their prospects and exploitation, particularly in the case of Hyena.

(iii) from December 1st until the end of the war:
December 1st saw a split of Daffodil into its component Luftgau keys (Luftgau XI-Daffodil; Luftgau VI-Wallflower; Lgau. VII-Aster; Lgau. III-Gentian; Lgau. VIII-Violet; Lgau. XVII-Foxglove).

From this date until the end of the war, the exploitation of the German keys, which now properly speaking included the Western keys as well,* became progressively more difficult. This was not merely due to key complications and compromises, but also to the security measures and devices of the Germans.

1·8093 The First Phase

Cockroach was soon added to the list of those keys which the Watch broke currently and usually inexpensively as a matter of day to day routine.

Daffodil was more unwieldy, and tended to be neglected a little after the opening of the Second Front, but it too soon became recognised as a bona fide Watch key. Traffic totals were enormous, and new groups of cribs appeared, including a vast family of Flubels (Flugzeugbelegungsmeldungen) from different aerodromes scattered about the Reich. Daffodil breakers were divided into two classes - those who plunged deep into the blists to pick out such messages, and those who were content to take the cautious but stubborn line of exploring morning and evening Predictions, cribs that could be identified with some certainty, and could be worked on with little imagination. The total amount of labour involved in breaking Daffodil was high, but then the measure of success achieved was high also.

Unfortunately this success did not spread to Hyena, which was examined from the start mainly in the Qwatch. We expected to be able to break an average of two days a week, with a few extras at times when Red was compromised and when Red cribs would pass on the Luftflotte key. The only Hyena crib during this period was the Reichspruch, and this was so dingy over long periods that re-encodements provided the best way in. Re-encodements had been investigated for the first time as early as April 1944, when messages passing out of the Luftgau XI area on the Luftflotte Reich stars, were systematically examined. Re-encodements did not have the same time of origin, the Red or Hyena messages coming as late as twenty-four hours after the Daffodil. This meant that the Daffodil version of a Red or Hyena message could only be identified by length and routeing. The idea at this time was to break recalcitrant Daffodil days via Red, and then to break Hyena via Daffodil. By the end of July, Daffodil was easy to break and the first step in the process could be eliminated.

1·8094 The Second Phase

The introduction of Reflector D on the German Air Keys on August 1st did not affect Daffodil at all, and the position on Cockroach was no more difficult than before, with the Gefechtsberichte remaining firmly on Reflector B. The position on Hyena was made much worse, however, since the Hyena versions of the Daffodil re-encodements were almost all on Reflector D. Luftgau VII still continued to use B on the Luftflotte Reich star, and by dint of much sweat and tears, the Hyena D for the first period was broken on a Travemünde

* See the History of the Western Air Keys for further details.

signature, but this luck was too good to last, and we could not expect it to be repeated every time. Even when the D was recovered after the Hyena key had been broken on the Reichspruch, the Daffodil re-encodements were very difficult to deal with, and new cribs like the "Burbelsatz", which appeared at the end of September, had a very short life.

In October, after many ominous threats, Daffodil produced its own Reflector D, but the amount of traffic sent on D was never very high. There was also some Enigma Uhr traffic, but here again owing to its sparse distribution the problem was kept well in hand. Cockroach remained steady despite a fair amount of D and Uhr. On the whole therefore, by the beginning of December, the problem of D seemed well in hand, except on Hyena, which was difficult enough anyway, but despite our successes no one was foolish enough to paint pictures of a rosy future.

1·8095 The Third Phase

The split of Daffodil into its constituent Luftgau keys on December 1st was a natural development, which was only surprising in that it had not happened before. Even after the change Daffodil remained much the biggest key, accounting for 500 messages or so each day. Of the other Luftgau keys, four - Wallflower, Gentian, Lily (which had been in existence the previous month as well) and Aster - were soon under control. Wallflower in particular proved very amenable to Watch treatment. Snowdrop, Violet and Foxglove never passed out of the research stage, and all proved very difficult. Little was known about Clover, the key of Luftgau I. The Snowdrop of these days had little continuity with the Snowdrop which had been broken so regularly earlier in the War.

Unfortunately no sooner had this group of Luftgau keys begun to look exploitable, than the Germans began to use wahlworts in a far more systematic and formidable way than ever before. This was particularly serious in its effects on the breaking of keys like Gentian, where the only line of attack was via short addresses or signatures, usually multi-versional, which became prohibitively expensive when allowance had to be made for wahlworts of uncertain length.

Re-encodements went up in value. Hyena was given quite a new lease of life by regular re-encodements from Wallflower, and some of the dingy, cribless Luftgau keys like Violet or Foxglove came out occasionally on re-encodements, usually discovered by Sixta. Early in January, a determined effort was made to spot and tie up re-encodements in a combined operation between the Watch E.P.'er and the Qwatch. Likely re-encodement candidates on Daffodil were marked by the E.P.'er, and returned by Hut 3 as quickly as possible. They were then looked at by the Watch, if they were operationally important, and passed on to the Qwatch (usually the Watch party in the Qwatch, which paid special attention to these re-encodements) if the Watch had no time to deal with them. The scheme resulted in some gratifying successes, and was just beginning to get really under way when the W/T complications of February 1st added to the problems of Hut 6.

Even without this new horror, the Luftgau keys were becoming sufficiently difficult to test our resources to the

maximum. In February, almost the whole of Lily went over to Reflector D, Gentian took to using Enigma Uhr, Aster went over to D and Uhr on February 10th, while the frozen runways, which had given us our only Snowdrop crib, thawed with the promise of an early spring. By dint of strenuous effort, hold was kept on Aster and Wallflower, and re-encodements from Wallflower to Hyena provided plenty of work for plenty of hands without producing much in the way of reward. Gentian, which had increased in volume as a result of the Russian drive on Berlin, was broken for two days at the beginning of March, but this was its swan-song. Wallflower ended with a flourish, passing a group of quite powerful Wasp cribs, before the Allies overran the area of Luftgau VI.

The final fortnight of the war saw the total disintegration of Hyena. Several keys were in use - the compromised key, two replacement keys, and some emergency keys. Genuine Hyena was a very small remnant at the beginning of May, and only Aster, of the Daffodil offshoots, ended the war in a blaze of glory. A re-encodement broke the second April D period, and a windfall arrived at the end of the month in the shape of a complete week's keys in a Jaguar message.

The story of Cockroach and Daffodil in this last phase of the war is not quite so gloomy, but marks quite a sharp decline in our fortunes before December 1st. Daffodil was made far more difficult to deal with by the encoding of call signs on February 1st. The identification of the Flubel messages became very difficult without callsign help, and though we built up a detailed picture of the distinctions between the different aerodrome reports (length, gap between G.T.O. and T.O.I., average G.T.O. etc), it was always changing, and impossible to keep up to date. Daffodil provided considerable interest for the cryptographers in the final period. Although the Allies poured into Central and Northern Germany, and overran the German aerodromes one by one, two Danish stations, Hjllsum and Hörnum provided a long run of Daffodil breaks until on May 3rd the crib frequency died and was heard no more. The story of Cockroach is more complicated. An increase in the use of Reflector D in the early days of 1945 was serious but did not affect our breaking powers. At the beginning of March Cockroach was renamed Wasp because Fliegerkorps IX had taken over control of the Jagdkorps I network, and its history is told more fully in the section on the Western Air Keys.

One new arrival in this last phase was Chimpanzee, the key of Luftlotte X, an organisation mainly concerned with the training of Air units. It was broken for the first time on a crib which had previously passed in Blue, a break which revealed the wide distribution of the key. A number of successes were scored until it too fell a victim to wahlworts and dingy and dying cribs, not however before it had provided a welcome re-entry into Foxglove. An odd re-encodement from Red in February did not clear the crib position, and by March the Germans had more to think about inside their own country than the training of new G.A.F. units.

1·810 THE EASTERN AIR KEYS

1·8100 General

The invasion of the Soviet Union, forecast by Enigma decodes on Rocket and Red, led to a great increase of traffic on the general G.A.F. key. The percentage of Eastern Front traffic was high, and continued high even after the splitting up of the key in January 1942. The amount of Eastern Front traffic relative to the total amount of Enigma traffic remained high until the end of the war, for it was on the Eastern Front that the largest German armies were contained and driven back until the end of the struggle. The importance and urgency of breaking this mass of Russian traffic varied greatly at different periods of the war. At some stages in the war, the traffic was regarded as being operationally important. Beetle was broken in C.R.1. currently with a high sense of urgency during the German drive on Moscow in 1942. Hedgehog, the G.A.F./Army liaison key in the area of Luftflotte 4, was broken in the Watch in 1943 but this was rather because of its breakability and the shortage of work in the Watch than because of its urgency. In the last weeks of 1944, Mosquito was given a lot of careful attention, and profited from the use of the new D-breaking machinery. In 1945, the last phase of cryptographic activity was centred on Ermine and other remnants of the Eastern Front keys. But on the whole, the Eastern Front from the point of view of Hut 6 was a subsidiary front. It never claimed the attention given to the African or to the Western Air keys, and the weight of Allied bombing on Germany obviously gave the German Air keys a more direct significance.

The same general story that applies to the other fronts applies to the Eastern Front as well, the story of increasing difficulties due to the German use of Reflector D and similar technical devices, and also to the increasing complexities of the German W/T and callsign system. Mosquito, a large and important key in 1945, suffered especially from Reflector D. The callsign problem made it very difficult to sort out the continuities of the Eastern groups, and the result of the mix-up was the wide range of keys, named after Counties or American States, which could not finally be identified. The keys were compressed into the relatively small area, which was the sole remains of the vast empire of the Third Reich.

Although the general story holds, there were certain other difficulties in dealing with the Eastern Front, that gave it characteristics all of its own. The first of these was the size of the Front. It was only possible for the Germans to treat the Eastern Front as a unity when they were driving forward and carrying everything before them. The Russian Marshals were able eventually to carve up the front into sectors by their swift and sharp drives towards the German and Polish borders, while the Red Armies in the South burst across the Balkans to Czechoslovakia and Austria. At the end of the war, we were dealing with two different sets of Eastern Front keys, those concerned with the Northern (Germany and East Prussia) sector and those with the Southern (Balkan and Austrian sector. Ermine had concerned with the Balkan and Austrian sector. Ermine had touched Gadfly in the South; Mosquito had touched Hyena and Lion in the North.

Because of the size of the Front, units were constantly being moved from one area to another, and this led to a certain amount of confusion about keys. Beetle began, for

instance, by being the key of Fliegerkorps VIII, but when Fliegerkorps VIII was withdrawn in May 1942 from the Moscow Front to the Crimea, Beetle became the key of Luftwaffen Kommando Ost (later changing again in May 1943 to become the key of Luftflotte 6) while Skunk, first broken in May 1942, became the Fliegerkorps VIII key. Keys would "amalgamate" for a month and then separate again - such as Hornet and Ermine in 1943 or Gorilla and Ermine in 1944. Keys would flourish and disappear. Hedgehog, the special operational key in S. Russia, was perhaps the most important key to do this. On the other hand, new keys came into operation quite late. Luftflotte 4 did not use its own key, Gorilla, until September 1944. It had previously passed mainly Red. The decline and fall of Red in the late summer of 1944 produced quite a spate of new Russian keys. It was always difficult to keep a hold on all the keys at the same time. For some occult reason, it was particularly difficult to break both Beetle (Luftflotte 6) and Mosquito (Luftflotte 1) at the same time. Some keys were never broken at all. These included not only small and unimportant Geschwader keys, like Rabbit or Badger, which abounded on this Front, but at least one quite important G.A.F. key on the Central Front (Puce), which passed quite a lot of traffic in 1944. Our hold on the East was never as complete as our hold on the West. Interception difficulties were perhaps the most important reason for this, but in addition, volumes of traffic would fluctuate alarmingly, and continuity over a period of years was very difficult to establish. Nearly all the keys had surprising changes of fortune, particularly the two most important, Beetle and Mosquito. Our record on the Luftgau keys, Foxglove and Orchid, was much better, though there were more re-encodements in these cases to assist our efforts.

It was not only keys that changed and fluctuated. Cribs had a fantastic butterfly life, some of them being very good for short periods then dying ignominiously, others were there for the duration, but moved disconcertingly from one key to another. The famous Befehl and Besan, archetypal cribs, were usually sent on Red, but they appeared in half a dozen or so other keys as well. Zusauf was a most steady crib, but always inclined to be fickle in its loyalties. In 1942 and 1943, Skunk Wetter had passed indiscriminately on Red and Skunk, and had broken both keys, not always breaking the one that was intended. Flak M.V.M. moved in August 1943 from Orchid to Weasel. In February 1944, Vordere Linie, a Beetle crib, passed on Skunk every fourth day, and eventually appeared on Skunk regularly. Such "crib vagrancy" was often as valuable in breaking keys as were re-encodements, though the value of the latter in the overall picture, particularly in 1945, cannot be over-estimated. Standard cribs, re-encodements, and the short messages which were sent when all was quiet on the Eastern Front, or at any rate on a very small part of it, were our chief stand-bys.

Because of these changes, there had to be particularly close collaboration between Hut 6 and Sixta in dealing with the Eastern Front. Sixta experts kept the study of the Front alive at a time when broken days were few. And there were times when the whole front seemed to be stricken with decay. This was particularly so in June 1944, when traffic totals were falling catastrophically, and frequencies disappearing chaotically. A Sixta re-encodement was one of the few hopes left to the cryptographer. It was only when traffic totals were really high that a sturdy independance could be maintained, and such periods never lasted for long.

1.8101 The German Advance

During 1941, there were many Eastern Front cribs on Red, and in the split up of keys in January 1942, some of the cribs survived. Hornet, the key of Fliegerkorps IV, passed two such cribs, Czech Wueb and Befehl. In January, a stecker repeat made Hornet particularly easy to break, twenty-six days being a very good total. Hornet continued to be easy in February and March.

Beetle, the key of Fliegerkorps VIII, was first broken on a chancy re-encodement from Red on March 7, 1942, which won a close race from a weather crib that had previously passed on Red, and whose continuity had on that very day been noticed by both cryptographers and Control. "Beetle Weather" thereafter broke many days, and was the standard crib until Fliegerkorps VIII left the Moscow Front for the Crimea in May 1942. This withdrawal led to the change of key distribution mentioned earlier. Skunk, the new Fliegerkorps VIII key, was broken for the first time in May 1942. It fitted into the Southern and not the Central Sector.

Mosquito, the other Central Front key (Fliegerkorps I, later Luftflotte 1) was not attacked very strenuously, even though it passed one old Red crib, Lett Wett. The reason was that traffic totals were very low.

Foxglove, the key of Luftgau Ost, later Luftgau XVII, was not broken until March 1942, when a providential stecker repeat revealed a number of tuners, of which the most likely crib was the "Glovespruch". There were signs of other cribs, however, and Recce messages were re-encoded from Red and Gadfly during the month of May. On the whole, however, though Foxglove was quite important, it could not be given high enough priority to compete with the African and Mediterranean keys, which had then reached their peak demand.

1.8102 Key Repeats

In the same month that Fliegerkorps VIII left for the Crimea, Hornet became terribly difficult, and was banished in disgrace from C.R.1. The Eastern Front seemed to be becoming impossible. A great recovery in the East came about from a wealth of key repeats, which not only enabled us to make up ground on the slipping keys, but paid handsome dividends in opening up the way to the breaking of new keys. What was perhaps most important of all, it was now possible to break solid blocks of days, whereas running on the limited number of bombes available could have produced at best only a limited number of breaks on this Front.

In June, for instance, it was possible to get into Skunk, the new key of Fliegerkorps VIII, by using the wheelorder and ringstellung of May Hornet, and the stecker of May Snowdrop. To get into May Hornet, it was necessary first to break the June Primrose, which was repeating wheelorder and ringstellung. In such a roundabout way, driving at keys of both months, it was possible to break a new key. Other keys to be broken on key repeats were Mosquito, broken on a key repeat from Cockroach, and Weasel, the key of Flak Korps I, on a key repeat from Daffodil.

August was the dominating month for key repeats, and without them the Eastern Front keys were very much of a Research proposition. There was a lull until December. This was the time of the fierce German onslaught on Stalingrad and the Caucasus. By December, when we had full use of key repeats again, the Russians had started their

great counter-offensive, and the war had turned. We also reaped a rich harvest in December, when Foxglove, Primrose, Celery, and Beetle formed a useful quadrilateral. The grip on Beetle did not long outlast the repeat, and the only other breaks on Weasel and Skunk were gained after great effort and perseverance. There were occasional cillies on Mosquito, which kept the key alive, and a new key appeared in the region of Luftwaffen Kommando Don. It was first broken in February 1943, and was called Ermine. It proved in effect to be the key of Fliegerkorps I, Mosquito now having been taken over by Luftflotte 1. Odd breaks were made on these keys in Research during the early months of 1943, but cribbery on the Eastern Front was always difficult because of interception diff-iculties, however much cover was put on, and also because of lack of bombe time for Research keys. There were however striking changes, which began on March 1st, when the Luftgau keys split up, and Foxglove produced seven components, corresponding to the different Luftgaue on the Front. This might have been a mortal blow, had it not been noticed that different Luftgau keys came out in groups, even though they had different discriminants. Clover, Foxglove and Narcissus came out on the same key, and Orchid was partnered with Daffodil. Clover was the key of Luftgau I, Orchid the key of Luftgau XXV. The investigation of this tangled set of twins and even quadruplets is described more fully elsewhere. Certainly it gave new life to the Russian Front.

1·8103 Hedgehog

The last burst of Watch activity on the Eastern Front as a whole came from their exploitation of Hedgehog, used as a general operational key on the whole of the Eastern Front, and replacing in most cases the local key of the Fliegerkorps. This key, along with Porcupine, a similar animal, was exploited at first by Research, but in May 1943 it was sent to the Watch. It stayed there until the end of August, when it split up again into its constituent Fliegerkorps keys. It was a very interesting key to deal with, offering a battery of short reports, most of them routines, known as the "Storchs", and what was much more valuable, a regular daily re-encodement from Red, known as the Luftflotte 4 R.E. Even when the message did not turn up on Red, the Watch could recognise the message on Hedgehog, and fit in the various beginnings - Luftflotte 4 unterstützte, bekämpfte, or merely führte. The re-encodement began to be sent also on Orchid, which was in consequence transferred to the Qwatch, and even on other small groups as well. All the June Orchid days were broken by this means. On one occasion at least, Hedgehog was rather less monotonous. It obeyed the G.A.F. Ringstellung Rule, and on July 24th was broken by hand, with a good cilli to make the going. It was with a good deal of regret, that the Watch said goodbye to the Eastern Front, when on August 1st the re-encodement was sent on Hornet and Ermine. From this time onwards, with one short exception, the breaking of the Eastern Front keys was a Research proposition.

1·8104 The Heyday of Research

As a Research proposition the situation was made a good deal easier by the disappearance of Hedgehog and the continued sending of the R.E. on Red and the different Fliegerkorps keys. So long as this lasted, the fortunes of the whole group were high. There were also Flugsi re-encodements from Red to Orchid, and Rundsprüche which passed in Hornet and Red. A good example of the measure of success that Research achieved at this time is seen in the week ending August 27, 1943. Nine Hornets, three Weasels, eight Orchids, six Foxgloves, five Ermines, and three Skunks were

broken. If there had been more bombe time, these figures would have been repeated more often. Difficulties of traffic analysis arose with the abandonment of discriminants on November 1, 1943 and the experiment was started of a composite Eastern Front blist sector by sector. This was valuable also in view of the increasing coalescence of the Southern and Central Fronts. It had been impossible earlier in the year to make a concentrated attack on Beetle and Mosquito, but now the Germans began to assemble some of the forces of Luftflotte 6 (Beetle) and Luftflotte 4 (Red) at common points of importance, and there was also a much closer inter-linking of Beetle and the Hornet/Skunk set-up. The two most active Beetle groups passed a considerable amount of Skunk. Beetle itself was broken on a re-encodement from Red on October 27, 1943, and it was possible with the help of cribs to get into a few of the other days. Mosquito remained an unsolved problem until a re-encodement from Beetle, a four-teile message on December 5th, broke the key for the first time for over six months, and revealed enough cribs to prepare the way for further exploitation. Traffic soared with the Leningrad offensive. Eventually decodes produced one valuable and interesting crib, called at different times Deck, Knob o' Garlic and Ventriloquist. These names were code names (Decknamen), which represented numbers and references, chosen from a list of about a thousand words. Two of the earliest to be chosen were Knoblauch (Knob o' Garlic) and Bauchredner (Ventriloquist). The validity of cover names lasted approximately for a month, so that with each change of allocation, the name of the crib had to be altered, until it got the composite name, Deck. Code names formed the bulk of the messages, and considerable ingenuity was required in breaking them. The Crib had previously passed in Red, a characteristic example of "crib vagrancy". Other Mosquito cribs were found, but successes faded out by the early summer of 1944. At the time of D Day all the cribs were dead, and Beetle too was in an unbreakable condition. A good deal of attention was paid to the two keys, in view of the possibilities of a large scale Russian drive in the East to synchronise with the Allied landings in the West, but June 1944 was a singularly black month for the Eastern Front as a whole, the lack of success contrasting strongly with the striking exploitation of the Western Front keys.

In the meantime, the period from 1943-4, saw many other changes in the anatomy of the German W/T system in the East. On September 1, 1943, Foxglove (Luftgau XVII), disappeared, and the bulk of Luftgau traffic now passed on Orchid, Gadfly and Red. Orchid was for the most part easy, until interception difficulties ruined effective breaking. The highlight was a memorable forty-eight hours in October 1943, when seven breaks were accounted for. As the months went by, the alignments of Orchid became more interesting. It became bound up with the Balkan keys, and had occasional re-encodements into Gadfly. Finally it was swallowed up in the autumn of 1944 into the maelstrom of Central Europe.

Attempts to get into Puce, or Gorse (Luftgau XXVI) were much less successful, despite occasional bursts of powerful but abortive cillying. Weasel was broken in patches. The Fliegerkorps keys had varying fortunes. Hornet disappeared early in 1944, and Ermine was broken quite regularly in the spring of that year. In fact, it was the only Eastern Front key to be well in hand at the time of the opening of the Second Front in the West.

1.8105 The Problem of the Luftflotten

On July 1, 1944, Red was compromised and the different Luftflotten took to their own keys. The Luftflotten on the Eastern Front were

Luftflotte 1 . . . Mosquito;
Luftflotte 4 . . . no key of its own, as far as was known;
Luftflotte 6 . . . Beetle.

This compromise of Red marked the beginning of the break-up of Red as a general key, for, although there was a recovery, a further compromise two months later, left lasting disintegration. In July, the traffic of Luftflotte 4 was sent out on the Skunk key, and the veteran crib Zusauf enabled us to make our breaks. In September, Luftflotte 4 used its own key, Gorilla, which was in use until the end of the war.

The Luftflotten were closely inter-connected, and all passed a fair but varying amount of Red traffic. Mosquito was at first more tractable than Beetle, owing to the occasional appearance of old cribs like "Einsatz". In August, however, the tables were turned. A re-encodement from Red broke Beetle of the 16th, and revealed some grounds for increased confidence. Traffic from Luftflotte 1 to Luftflotte 6 had addresses which were cribbable, though only temporary in nature, and there was a residue of Flivo traffic, which while sporadic in appearance, was workable in content. It was on re-encodements from Beetle that we were able to get into Mosquito and Gorilla early in September. Both keys had their own individual lines of attack - Gorilla by the Zusauf, Mosquito by the use of ex-Red cribs - but the re-encodements from Beetle were essential preliminaries to further cryptographic drives.

The really complicating factor was the appearance of Reflector D on the Eastern Front. By the end of September (the date of the disappearance of Air Research as a separate body and its absorption in the Watch), all the old Red cribs on Mosquito were sent with Reflector D. Gorilla too had its D, and the first Gorilla D was broken without a crib by the new Bobbery method, described in the technical volume. Beetle alone seemed to be entirely on B, and could be handed over to the Watch for current breaking, chiefly on routine Gefechtsberichte. Gorilla too became a Watch key. Mosquito sulked behind the scenes, and was never amenable to current treatment. However, like all situations on the Eastern Front, this situation did not last for long. Mosquito revived at the end of October, and, because of the Russian offensive, became of some operational urgency. By the law of compensation, Beetle relapsed, and the standard Geraeteklarmeldung disappeared. This time, however, the law of compensation did not bring about perfect equilibrium. Relapses, revivals, and short spurts of success on both keys continued until the end of the war. Mosquito profited from the development of the new D-breaking machinery, and the Erdlage re-encodements from Lion or Red were suitable fodder. The link-up with Lion shows the complete reversal of fortune on the Eastern Front. At the same period, Gorilla was linking up with Gadfly and Ermine in the lakes and mountains of Hungary and the approaches to the Austrian borders. The fortunes of Gorilla were variable, but on the whole sound. In September 1944, it absorbed Ermine, but had to compete with Red II, which was also used in the Luftflotte 4 area. Competition with Red persisted: Gorilla was sound when it passed Zusauf, tricky when Red took the crib over. Even Zusauf was not missed when Befehl and Besan made their sporadic appearances on Gorilla, and the cobwebs were dusted from their folders, which had long lain buried in forgotten archives. Between Luftflotte 4 in the South and

Luftflotte 1 in the North, Luftflotte 6 (Beetle) fluctuated both in traffic totals and in exploitability. It was just kept alive in December by a mysterious stecker repeat with Cockroach, and afterwards began to use Reflector D. By the end of January 1945, Reflector D was the big bogey everywhere.

1.8106 The End

On February 1st, the Germans introduced the system of encoded callsigns and changing frequencies, and although some of the Eastern Front keys continued to use the old routines, the general effects of the W/T picture in the East were very depressing. In particular, a number of groups now existed, which had recognisable continuity (chiefly by discriminants), but which could not be precisely identified. Such groups took County names (e.g. E/Suffolk) and later the names of American States (e.g. E/Ohio or E/Maryland). Frequent compromises on the Eastern Front and the extensive use of Reflector D, made the position very complex, but it is true to say that much of the cryptographic interest of 1945 centred on this very difficult field. Properly speaking, we were faced with two complexes, first the South-Eastern Complex, consisting of Luftflotte 4, with Fliegerkorps I and II attached, and second the Eastern Complex, consisting of Luftflotten 1 and 6 with Fliegerkorps VIII.

The South-Eastern Complex represented the remains of German Balkan power: the three units, formerly so powerful, were now squeezed into a relatively small area. The communications of Luftflotte 4 were complicated in February by the use of "Pink" - identification dubious - for communications to Luftflotte 4 from the higher authorities. Gorilla was still used in the dealings of the Luftflotte with its subordinates, and it decoded also the last remnants of the Gadfly networks.* Locust was used by Fliegerkorps II, and took over the remains of Yak. Ermine, the key of Fliegerkorps I, had had a very varied recent history, but it was breakable on its ancient weather message, whenever it appeared. On the whole, some hold was maintained on this South-Eastern complex until the end of the war, and if the war had been prolonged, we could still have registered some successes. In May 1945, Gorilla and Locust were both repeating the April key for part of their traffic, while the last key to be broken by Hut 6 was Ermine. Even after Grand Admiral Dönitz had agreed to unconditional surrender, a small party of cryptographers still wrestled with this small but interesting tangle of keys.

The Eastern Complex proper was so complicated that it could only be tentatively mapped out in the broadest outlines. Beetle, the key of Luftflotte 6, was broken by D-breaking machinery, and Skunk, the key of Fliegerkorps VIII, dependent on Luftflotte 6, followed shortly afterwards. Skunk was almost 100% D, and partially Enigma Uhr as well, but it ended in a blaze of glory. Both the third and fourth D periods of April were broken, and as May repeated the April key backwards, we should have been able to read the traffic for as long as the Germans continued to oppose the Red Army. Mosquito was less fortunate, and was mixed up with both Beetle and the County keys. A new key, Moth, made its debut, when Fliegerkorps II left the South East for the Northern sector. This wealth of keys produced a welter of re-encodements, providing far more work in April and early May than Hut 6 was capable of dealing with. The extent of Reflector D on the minor keys made

* See the Report on the Mediterranean Keys.

all shots on the bombes something of a gamble. And in the last days "crib vagrancy" was particularly marked. Cribs would be searched for on any Eastern Front blist, and in the confusion, no-one knew quite which key was being broken. Even re-encodements from Army keys came into their own, and Avocet/Skunk re-encodements appeared on several occasions. Despite all the havoc, the efforts and the patience of the cryptographers were still not quite exhausted on May 8, 1945.

1·811 THE EASTERN ARMY KEYS

1·8110 General

The ebb and flow of battle on the Eastern front was rarely the sole reason for the great fluctuations in the volume of wireless activity which were the most marked feature of interception in this campaign. There were periods of static warfare when traffic was passed over the air in some quantity; and there were great and fierce battles which produced no W/T reaction whatever. The reason lies in the extensive landlines which the Germans kept as far as possible constantly in working order, and also in the Fish links from O.K.H. to the Armies and Heeresgruppen which were set up at a fairly early date.

1·8111 Initial Advances, June - December 1941

When Hitler invaded Russia on June 22, 1941, traffic began at once to be intercepted in some quantity and before the end of the month one of the two main keys, which were named Vulture I and II, was broken on cillies. In the following months there were occasional breaks until a big increase in cillying in September led to frequent and early breaks for a long period. Cribs soon appeared, for the Heeresgruppen and Armies were all sending their operational reports by wireless, and there were often cillies on the crib messages. The Vultures provided traffic at the highest level, which would have been of great operational urgency had it been dealing with a front on which British troops were engaged. As it was, it was of extreme interest but not of great urgency.

Other keys of less importance but with some volume of traffic were also identified at this time. There was Kite, a general supply key, of which one day was broken before the end of 1941; and Kestrel I, II, III, and later IV, the broadcast keys (Rundspruchmaschinenschlüssel) for the four Heeresgruppen on the front. It is clear now that a key of this type was part of the recognised equipment of each Heeresgruppe, but the use to which they were put changed in the course of the war. At the end in the West they were used for broadcasting intelligence of general interest derived from Y; but in the early stages of the Eastern campaign much of the traffic dealing with Army Air Force co-operation which later passed in the Air Flivo keys was sent in these Army broadcasts. In the autumn of 1941 many days of these keys were broken on cillies and on cribs. In fact with sufficient bombe time all days would have been broken without much difficulty, for on all the keys there were early cribs reporting on the number of messages sent and received during the previous twenty-four hours. During the early months of 1942 Kestrel traffic continued to appear in fairly small quantities, and the policy was adopted of breaking if possible at least one day per week, to make sure that the cribs remained unchanged in form.

1·8112 Quiescence, 1942-3

In January 1942 Vulture traffic dwindled to nothing, as a consequence of some stablisation of the front and widespread construction of landlines. The system of wireless communication was still available if required but it was only used when all other methods had failed. Presumably as a security measure, the W/T network was radically altered to the exclusion of

the series of stars used in the opening phases of the campaign. Instead the G.H.Q. Netz was extended, by which each Army and Heeresgruppe was allotted a receiving frequency and was thus enabled to communicate with O.K.H. or any other unit in the system by use of the appropriate frequency.

Throughout 1942 activity on the Netz was very low. In a burst of traffic one day in July there were enough cillies to break the day; and the same thing happened again in December. Then traffic totals in general rose steadily, and in particular there was daily a large amount from the beleaguered Sixth Army at Stalingrad. Another break on cillies showed us the form of some of the routine reports from this Army, and it then became possible to break on cribs a number of days before the eventual surrender early in February.

This was a good example of the opportunist methods that had to be used to exploit the unpredictable appearances of Eastern Front traffic. It was impossible to tell how long these bursts would last, and therefore one member of the Research Section always had the investigation of the Eastern Front traffic as his primary responsibility, in order that no chances of obtaining such valuable intelligence should be missed. Thus in March 1943 the Vulture parent observed a KR message with time of origin 0500 passing on the same frequency on four successive days and broke a day on the assumed beginner MORGEN-MELDUNG. This was the first of a spell of breaks of Central Front traffic, the units engaged being Heeresgruppe Mitte, A.O.K.2, and Panzer A.O.K.2. A.O.K.2 sent several routine reports of which the Morgenmeldung was the simplest to recognise and the most standard in form, and a remarkable feature was the fact that the range of forms used on these messages in March-April 1943 was precisely the same as when they had previously been seen in Autumn 1941.

1.8113 Spread of Use of Local Keys, July 1943 - December 1944

July and August 1943 saw a steady level of traffic from O.K.H. with a marked tendency to keyboard cillies which gave us several days. This time, however, the traffic provided no crib; and when next a Russian Front break was achieved in October, on one of the old A.O.K.2 cribs sent over the air on one single day, it was apparent that some change in the normal key usage had taken place. Only traffic passing between Heeres-gruppe Mitte and A.O.K.2 decoded whereas in July similar messages were coming out on the general key.

The tendency to use a local instead of a general key was seen again when in February 1944 a break was made into Owl, the key of A.O.K.17 in the Crimea. At the same time there were signs that the old Netz system of working was not proving entirely satisfactory, most of the units regularly active on the air using fixed line frequencies, although they had still their Netz frequencies available if required. This was a general development not confined to the Russian Front. Thus A.O.K.10 in Italy had special frequencies for communication with O.K.H. and a special key, Bullfinch, for use on these frequencies in addition to its normal Armee key, Albatross. Similarly A.O.K.17 had line frequencies and a special key, E/8532, for traffic to O.K.H; while there was a fixed frequency for communication between the Army and its controlling Heeresgruppe, H.G.A, on which the Armee key, Owl, was used.

Owl was an interesting colour to break, with several cribs of variable forms which required considerable judgement if they were to be employed sucessfully and inexpensively. Owl I was broken more often than not until May 8, 1944, the day before the German surrender in the Crimea. Odd days of the Staff key, Owl II, were obtained by the standard G-Tail technique.

Traffic still came in bursts from different parts of the front, but if two Armies began using W/T at the same time it was now more than likely that they would be using different keys. The general key was still in existence, for some cillies from Panzer A.O.K.1 at the end of March gave four or five breaks, of which some were obviously the Armee key (Pelican), while some decoded traffic from other parts of the Front.

In late June, July and August there was heavy traffic from the Northern sector of the front, with a number of different keys in use. In the resulting difficulty of identification keys were known as "Vulture 2924" or "Vulture 5393" according to the frequency on which they were used; the genuine Vulture key, the O.K.H. key for use in the East, was renamed Avocet to distinguish it from the many pseudo-Vultures. The Geheim Tail method of attack brought a number of breaks, which in due course revealed the key distribution and usage. Avocet, by far the largest, was used for communications between Heeresgruppe Nord and Heeresgruppe Mitte as well as among their subordinate Armies. Flamingo was used between O.K.H. and Panzer A.O.K.3, which gave us several days early in August on cillies. And several smaller keys which were not given separate names were connected with different armies on other parts of the front.

1.8114 The Final Spurt

Traffic fell suddenly for a week or two but rose again in September, and for two months continued heavy but very difficult to break. Drives on Geheim Tails sometimes staggered to allow for a final wahlwort, produced only isolated breaks, and it was not till the end of December that progress began to be made by means of routine messages. At the same time an entry was made into Avocet II, which proved to have a daily routine message of some value as a crib in spite of its addiction to wahlworts. This was the Feindbeurteilung, a 1C report from Heeresgruppe Nord giving an appreciation of Russian dispositions and intentions. During 1945 occasional breaks of Avocet II were made on this message, while Avocet I was broken with steadily increasing regularity, the routine reports from the isolated Heeresgruppe Kurland being the best of a large number of possible cribs.

The last fortnight of the war saw Avocet being broken as a full Watch colour by the Army Watch, the fronts being by then so confused that some of the units seemed to be facing East and West at the same time. By a turn of the wheel full circle, the German campaign against Russia ended as it had begun with nearly all active units on the air and using one general key, so that Hut 6 was able to provide a commentary on the last days as on the first.

1·812 GREENSHANK AND ALLIED KEYS

1·8120 The Main Features of Greenshank

There were times in the history of Hut 6 when we felt that the enemy was delivering himself into our hand; when one simply had to write out a crib which said the same thing every day it all seemed just a little too easy. One group of keys, however, never produced this reaction. They were under the direction of a signals officer who was clearly pitting his brains against those of the Allied Y Service and Hut 6 welcomed the challenge. For years Greenshank stood as a massive peak inviting assault, surrounded by lower hills which were surmounted in turn in the hope that they would prove steps on the path to success.

Greenshank, or Green as it was called in 1939 and 1940, was the key of the German Home Administration. Germany, even before the war, was divided into about twenty military districts (Wehrkreise), each with its H.Q. Each district was responsible for the recruitment of a Corps, which in time of war would be reinforced from its home area: and so the Wehrkreis administration was regarded as standing in place of the Corps. Hence the duality of nomenclature whereby the home H.Q.s were referred to as simply "Wehrkreiskommando I, II etc." or as "Stellvertretendes Generalkommando I, II, etc.,Armeekorps".

The Wehrkreis stations were linked by a wireless system which was extremely complicated long before the war. The operators were highly trained and well-versed in each others' foibles - "eingespielt", as they themselves neatly put it - so that traffic was dealt with speedily and with a minimum of queries and delay. The W/T system was designed to make interception as difficult as possible, consisting of a high-frequency Netz in which each station had one receiving frequency out of a possible twenty-six, which were allotted according to a clever daily-changing table, and a simple low-frequency network in which five or six frequencies served the need of all the stations. The change-over from high to low frequency was often carried out at short notice in the middle of a message. And the initial success of these tactics may be judged from Mr. Welchman's discovery early in the war, that while S.Y.G. had been unable to intercept most of the L/F traffic for lack of L/F sets the French had been concentrating on the L/F and were quite unaware of even the existence of a H/F network!

The complexity of the frequency system was one indication of the competence and discipline of the Wehrkreis wireless operators. There was some evidence that their cipher clerks were of the same standard, for there was a rule, normally not closely adhered to, that the length of one part of a message should not be more than 250 letters. Throughout the war it is believed that not a single Greenshank message was intercepted with more than 250 letters, and usually each part was as near 250 letters exactly as it could be. It was no uncommon thing to see a teil-message with a very short last teil, e.g. 3 Tle. 1T 249. 2T 250. 3T 6., where on any other network the operator would have committed a very venial breach of the rules.

Other remarkable features about the Greenshank traffic were its bulk - a steady average of 200-300 messages a day - and its obviously non-operational character. Most of the Wehrkreis stations did not work at night, there was little KR traffic, and

many messages were sent several days late. Greenshank was not a key likely to provide information of operational urgency. No single message was likely to be of much importance; but it was hoped that steady breaking would give a wealth of intelligence on minor matters of administration and supply which would enable a clear picture to be drawn of conditions and troop movements inside the Greater Reich, just as Falcon in 1943 and 1944 accurately sketched affairs in Wehrkreis VI.

1·8121 Breaks, 1939-1942

Green was broken on the old indicating system in October 1939 and several times afterwards until the change of indicators in May 1940. At this time the traffic was largely practice, and it was not till November 19, 1940, a day which was broken by hand on cillies, that a good sample of Wehrkreis traffic was read. This break revealed no crib, and no more cillies appeared, so that no advance was made.

During 1941 there were periods when the Wehrkreis network was not intercepted owing to lack of sets, but towards the end of the year traffic totals were high again and a number of attempts were made to break on what were later called Berlinismus menus - from the habit of the Berlin station of stepping its outside indicators alphabetically or along the keyboard with gaps of one, the intervening letters presumably being the inside indicators. Thus one would find such sequences as

1.	AJS	QJR		1.	QAY LTA
2.	CLU	ZOL	or	2.	EDC KGO
3.	ENW	HHG		3.	TGB BYL,

the inside indicators in the first case being assumed to be BKT, DMV, FOX, and in the second WSX, RFV, ZHN. None of these shots succeeded, and strong though they seemed, the impression grew that the basic assumption must be wrong.

During 1941 the Wehrkreis traffic stopped discriminating, and when therefore some cillies began to appear on a small extension of the Wehrkreis network in Czechoslovakia, there was considerable doubt as to whether they were on the main Green key. One day was broken and the key failed to decode any of several samples of traffic taken on the main network; and it was therefore assumed that the Villach extension used a separate key. Two months later, however, it was discovered that the Orange and Mustard keys had a variable ringstellung, and a Green message was therefore decoded on the Test-Plate in all positions on the March key. It came out - and proved to have the original ringstellung ! The remainder of the traffic was then tried and about half decoded on all six permutations of the wheelorder. The rest had to be left unbroken.

From an analysis of the decodes and duds it appeared that there were two keys, the identity of the key being revealed by summing the last two figures of the time of origin. Further, the day had been split into six unequal periods in such a way that roughly the same volume of traffic would be encoded in each permutation of the wheelorder. The permutations were not in any obvious order like the ABC, CAB, BCA order which later came into general use. And there for the time the matter rested. The decodes were most unpromising, for there were no routine messages and the addresses and signatures were usually buried in the text of the message. This no doubt accounted for the failure of a programme of addresses produced on the evidence of the 1940 break

coupled with a crash analysis of the traffic from each station taken over a period of several months. From this it had seemed that the beginner AN STELLV (X) GEN (X) KDO (X) ROEM was most likely on messages from Berlin, and a programme of twenty or thirty of such shots had been run in the early part of 1942 without success. Further, the failure of the Berlinismus attempts was probably due to the fact that some of the messages used in each shot had been in a different wheelorder or key from the others.

1·8122 A Blank Wall

From this time until the middle of 1943 Greenshank remained a problem offering no hope, no glimmer of hope, of solution. Then re-encodements, thrown up by a general comparison of times of origin, began to appear, first from Mallard, which was very rarely broken, and then in the autumn from Falcon, which was coming out with fair regularity. Clearly the re-encodements were not straightforward, but nevertheless some quite good shots were produced which aroused some suspicions by not coming out. Then on October 10, 1943 a re-encodement appeared which gave a first-class answer, and when several consistent versions had been failed it was assumed that some change had been introduced into the machine. Versions were therefore run assuming in turn a twist of Reflector B, Reflector C, and the wheels and Reflector combinations of the Naval machine, all without success.

Then on Christmas Day came the news in a Red message of the intended introduction of Reflector D on Red on January 1, 1944. Perhaps the new Reflector was already in use on the Wehrkreis ? At this point came information that a Pole had deserted to us in Italy who had at one time served as a cipher clerk in some of the Wehrkreis stations, and an interview was arranged in the hope that he might be able to give us the answer.

1·8123 Inside Information

By January 15, 1944, the date of the interrogation, two wirings of the new Reflector had been recovered and there was considerable speculation as to its nature. Gefreiter Pziuara, however, could tell us nothing of the new invention, for he had been moved from Hanover in October 1942, after spending some months there and in Berlin. But he gave us some interesting details of the Wehrkreis practice.

Each encoder had two Enigma machines set up to two quite different keys called A and B. He decided which key to use by adding together the last two figures of the time of origin, and referring to a table on the key-sheet of the form:-

A	2	3	5	7	8	9	10	11
B	0	1	4	6	12	13	14	

Thus a message with time of origin 0721 would give the answer 2 + 1 = 3; therefore key A, and time of origin 1259 would imply key B. This table formed part of the key and changed every day.

The basic wheelorder and ringstellung for the day were given in charts in the form:-

	I	II	III	IV	V
1		14	03		23
2	07		01	19	
3	24	16	15		
4	13			11	20
5			08	17	11
.	.	.	.	.	.
.	.	.	.	.	.
.	.	.	.	.	.
31	14	01			25

Thus the basic wheelorder for the first of the month would in this case be 235 and the ringstellung 14, 03, 23, or as we preferred to say NCW.

The day was divided into six periods, 0000-1115, 1115-1330, 1330-1500, 1500-1700, 1700-1800, 1800-2400. The six wheelorder permutations were lettered:-

a = abc = Basic wheelorder
b = cab
c = bca
d = acb
e = bac
f = cba

One of these letters was allocated to each period by means of a further daily-changing table, e.g.

Day	0--1115	1115-1330	1330-15	15-1700	17-1800	18-2400
1	a	c	e	d	f	b
2	f	d	b	a	e	c

These measures ensured an even distribution of traffic between the two keys and among the wheelorder permutations, and made it quite impossible for anyone to tell from the outside either the key or the wheelorder of any particular message. The main points of the system had been guessed at following the break of March 1942, but the details were enlightening and perhaps rather depressing. If the Wehrkreis authorities had made such clever use of the standard Enigma, they would surely show no weakness in their employment of the new device which they had presumably introduced.

1·8124 The Mystery Solved

Re-encodements from Falcon came in a steady stream in the early months of 1944, and occasionally good shots were run on the ordinary bombes, and Reflector B "just in case". There was also at this time a revival of Berlinismus and of a similar indicator habit named after the station which developed it, Viennismus. Both types scored successes on Nuthatch, the key used on the southern extension of the Wehrkreis to Belgrade, and therefore the underlying assumption on which our menus were produced was proved correct. Early in February there was a day on which the Berlin operator excelled himself by producing at least fifteen different indicators of this type in the same period,

and proved to be on the same key by various repeats both of indicators and text: the failure of menus on these indicators removed any lingering doubts there may have been that our inability to break the Greenshank was due to a change in the machine.

It remained for Lionel Clarke, the relentless pursuer of the Greenshank, to demonstrate what that change was. On April 27, 1944 there was a re-encodement from Falcon to which a fairly complete and plausible solution had been fitted. He attacked this by the stecker knock-out method and broke the day in about a week's work, a well-deserved success after his years of labour. The break showed that Greenshank was now using Reflector D, as we had suspected, for the Reflector recovered had the fixed BO pairing. The next stage was to discover the period of validity of each wiring; on the Air keys one wiring lasted for ten days and if this were the case on Greenshank, then with the arrival of D-breaking machinery it might be possible for Greenshank to come out fairly regularly. Several shots were therefore run on days near the 27th, assuming the D wiring of that day. The only success was Greenshank B on the 27th which showed that only one Reflector wiring was used for both keys on any one day. The shots which failed were not by any means certain, and therefore the period of validity of each D wiring remained in doubt.

1.8125 The Last Phase: Statistics and Summary

The completion of Duenna and Giant, the reflector-breaking machines, at the end of 1944 enabled Greenshank to be run again early in 1945, although by this time the introduction of the "CY" device, by which the position of the left-hand wheel was altered in the middle of a message, meant that the maximum number of letters which could be at consecutive positions of the machine was reduced from 250 to 150. And as Giant required 200 letters of crib, it could not be used for Greenshank menus. But its use on Air jobs meant more time for Greenshank on Duenna. In January 1945 there were routine re-encodements between Falcon and Greenshank, and in spite of the tricks of alteration employed by Münster which was normally the re-transmitting station, Major Babbage, Lionel Clarke and others developed their technique of re-encodement to a point at which they could produce a stretch of over 100 letters with reasonable certainty in perhaps 20% - 25% of the cases. During February the re-encodements began to dry up though two final breaks were secured in March. However, January 1945 was left as the best Greenshank month, ever since the days of the old indicating system.

The following chronological table will perhaps give some idea of the stubbornness of the opposition (dates referring to breaks are underlined):-

Jan. 1940	Green of October 25, 1939 broken (first war-time break in Hut 6)
May, 1940	Change to Double Indicator System
Nov.19, 1940	Broken on cillies by hand
? Jan.1, 1941 or 1942	Introduction of six wheelorder permutations and two-key system
March 5, 1942	Broken on cillies (one key only)
? Jan.1, 1943	Introduction of Reflector D

April 27, 1944 — Broken by hand stecker knock-out by L.E. Clarke on Falcon R.E.: second key broken on bombe

Jan.5,7,17, 1945 — Broken on Falcon R.E.'s on Duenna or Auto-scritcher: on 5th and 17th second key on bombe

Jan.14, 1945 — Broken by S.K.O. by Major D.W. Babbage on Falcon R.E.: second key on bombe

March 6,7, 1945 — Broken on Falcon R.E.'s on Duenna or Auto-scritcher (one key only in each case)

Our methods of breaking depended upon the discovery of cillies, cribs or re-encodements and the Germans had orders not to send the first two of these, and to change the last in such a way as to make them unusable. It will be seen that in the five years from May 1940 to the end of the war eleven keys were recovered from re-encodements, two from cillies, and none at all from cribs. Such was the security of the Enigma when properly used.

1°8126 The Associated Keys: Falcon, Gannet II, Mallard

A number of keys were used on groups connected with the Wehrkreis system, and throughout the war the most determined efforts were made to break them, partly for their own sake, but more especially to secure a possible means of entry by re-encodement into Greenshank. The Greenshank key was not normally used for the internal W/T systems of the individual Wehrkreise, or for communication with stations outside the Greater Reich. Thus most of the Wehrkreise used Falcon (Heeres M/S) for their internal networks, while the extensions of the administrative network into Finland (Kemi), Eastern Poland and Russia, and Yugoslavia (Belgrade), used Gannet II, Mallard and Nuthatch respectively.

The Falcons are referred to in detail under the heading of "Western Keys". Falcon I, though a key of wide distribution, was chiefly used for traffic on the internal Wehrkreis VI network, and re-encodements into Greenshank occurred when a message from a station such as Bielefeld was sent to Berlin via Münster, the Wehrkreis VI H.Q., the first transmission being in Falcon and the second in Greenshank. Falcon II, the Staff key, was occasionally used as the Staff key to Falcon I in Wehrkreis VI, but, from July 1944, the bulk of the traffic came on the Wehrkreis network proper. There was no Staff key to Greenshank and Falcon II was generally used instead. This was extremely fortunate from our point of view, as Falcon II using Reflector B was breakable while Greenshank on D was not.

Gannet II was used between Berlin and Finland, and was first broken in August 1943 on a stray re-encodement from Vulture. Later breaks were made on Berlinismus, an address to the 20th Mountain Army in Finland, and on the beginning or ending known as "Siva" (SPRUQ IST VOM Date of an earlier day) which occurred on some of Berlin's messages. The quiescent state of the Finnish front normally resulted in only small quantities of traffic of low intelligence value. There were very occasional re-encodements into Greenshank; none of them proved of any value, chiefly because Gannet II could not be broken to order. One had to wait for a day of heavy traffic and then run a number of addresses and "Sivas".

Mallard was never broken with any regularity. There were perhaps four or five isolated breaks in the course of some years of traffic, but they revealed no way of holding the key. On September 1, 1944, the functions of Falcon and Mallard seem to have been interchanged or combined, so that perhaps the key broken under the name Falcon should more correctly be called Mallard. At any rate one of the keys seems to have gone out of use at that time, and Gannet II disappeared too, the traffic being sent in the Falcon-Mallard key.

1·8127 The Breaking of Nuthatch

The Falcons, Gannet II or Mallard, in spite of their close connections with the Wehrkreis system, were Enigma keys of the normal type with the usual three wheelorder periods. Nuthatch, the key used on the triangular automatic link between Berlin, Belgrade and Vienna, followed closely the Greenshank pattern. It was stated above that in 1941 Greenshank stopped discriminating. In January 1943 the main network began to use discriminants again, but the Belgrade extension remained as before, the traffic being known for want of a better name as "Non-discriminating Greenshank". An isolated break was secured on February 14th when the outside indicators of a teil-message were alternate keyboards, the inside indicators being correctly guessed to be the missing ones in the sequence. This break, the first success of Berlinismus, revealed that the "Non-discriminating Greenshank" was not using the main key: but it had little value apart from this, as very few messages decoded and they had no crib possibilities.

No progress was made for several months until three re-encodements from one of the Fish keys, Tarpon, were discovered by Sixta in the traffic of September 16th. After some difficulty the correct solution was found to one of them but the key decoded only the three R.E.'s and one other message, the three R.E.'s decoding on the same wheelorder, and the other message on a non-cyclic permutation. The remainder of the traffic, some 70-80 messages, seemed outwardly indistinguishable from the messages which did come out.

It was not until November that the solution of the mystery was found. Then two October days were broken on R.E.'s from Woodpecker, a key used in the Balkans apparently for teleprinter traffic, and broken at the time because one of the Wryneck cribs happened to be sent in it. Nuthatch, as the non-discriminating key was now called, was using two keys and six wheelorder permutations like Greenshank with the same method of distinction by time of origin. But the Nuthatch group did not play strictly according to the spirit of the rules, for the cipher clerks clearly arranged the times of origin of the messages in such a way that the vast bulk of the traffic on any day was on one key. By ill-luck on the September day we had broken the small key. Subsequent breaks were in almost every case of the large key, decoding 70-80% of the traffic. The residue was usually too small to be worth breaking.

From November 1943 to June 1944, when the wireless link disappeared, some days were broken in each month on "Siva", Berlinismus, and "Qef", an address used on some of the messages from Vienna to Berlin which said QEF HEER RUEST UND BEF DES ERS. The proportion which began in this way was small, but the form was invariable; so that occasional breaks could be expected if enough messages were run.

The intelligence value of Nuthatch was low. In spite of its close association with Greenshank there were few re-encodements between the two keys; and an early hope that the two Nuthatch keys, which used Reflector B, might be the same as the Greenshank pair which used D, was soon effectively disproved.

1.8128 Grouse and the Wehrkreis CQ key

Two other Wehrkreis keys were identified, which both used Reflector D. One, called by us Grouse, was used on an extension of the Wehrkreis system in Austria, North Yugoslavia, and Czechoslovakia, and, although it was never broken, near the end of the war two months' keys were captured without the Germans' noticing the loss. The key had a different Reflector wiring each day, but was in other respects similar to a normal Army key, i.e. all the traffic was in one key and only three wheelorder permutations were used. The German name for Grouse was the "Wehrkreis Fefu (Feste Funkstelle) Maschinenschlüssel", although as far as is known it was only used on the southern extension of the Wehrkreis which connected centres like Graz and Innsbruck.

Yet a third Wehrkreis key on D was that used for CQ messages sent out from Berlin. When these were Geheimekommandosachen they were encoded in Falcon II, and we read several of them in this key in the closing months of 1944. They either began or ended with a CQ serial number which said simply, e.g. SAMMELSPRUQ NUM SEQS ZWO FUENF. In dealing with such messages the Wehrkreis operators showed what for them was remarkably bad security, for they often referred to them in clear by the serial number. Sometimes a message would be received by Berlin and retransmitted CQ, and in such cases there was always an addition to the last teil of the message which was of course the serial number. So that on several occasions we were able to fit cribs to such additions, but when run on the ordinary bombes they did not come out. Since they did not decode on Greenshank or Grouse, one must assume that here was a third Army key using a daily-changing Reflector D.

1.8129 The Rôle of W.O.Y.G.

It would not be fitting in any account of the Wehrkreis group to close without mentioning the magnificent work of the W.O.Y.G. intercept operators and liaison staff. Only the skill and experience of the operators enabled them to take this most difficult network, and their work was only made possible by the brilliant feats of Malcolm Spooner, who, an almost legendary figure working in the small hours of the morning in his tiny office, could be relied on to break the various complicated systems of callsign and frequency allocation which the Wehrkreis authorities from time to time devised.